7DS Digital Instrumentation and Control Design Verification for Safety-Related Systems

The purpose of this appendix is to consolidate information regarding key design features of the safety-related platforms, and to facilitate mapping of applicable Design Acceptance Criteria (DAC), and Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) against that information. This appendix does not include any changes to the design as described in other portions of the COLA. This consolidated information is collected from various parts of the COLA (Tier 1 and Tier 2 of the COLA FSAR), the referenced ABWR Design Control Document (DCD), and various applicable technical and topical reports.

The scope of this appendix is limited to safety-related platforms selected to implement the design and functionality of the Safety System Logic and Control (SSLC) for the ABWR. The Field Programmable Gate Array (FPGA)-based platforms are used for the Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring System (NMS). The microprocessor-based platform is used for the Engineered Safety Features Logic and Control System (ELCS). The RTIS, NMS, and ELCS implement SSLC.

The platforms that implement the SSLC system have been designed in large part based on four essential design principles: (1) redundancy, (2) independence, (3) the need for defined determinism in data processing and communication, and (4) implementation of a diversity and defense-in-depth (D3) philosophy, as well as one subjective attribute–simplicity. The four principles and one attribute are embodied in the underlying basis of IEEE-603. The safety-related digital instrumentation and control (DI&C) platforms as described in Tier 1 Section 3.4; Tier 2 Subsections 7.1, 7.1S, 7.2, 7.3, 7.6, and 7.9S; and elsewhere in the FSAR satisfy IEEE-603 and thus the four principles plus one attribute. Conformance to IEEE-603 is explicitly described in each of the above Tier 2 sections.

Confirmation that the SSLC system platforms are implemented in accordance with the licensing basis is provided by Tier 1 ITAAC and the DAC hardware-software development process associated with Tier 1 Subsection 3.4B.

The consolidation of information in this appendix supports and clarifies the ITAAC and DAC resolution process for future use by those entities performing, reviewing, and approving the resolution. This appendix does not address conformance with all of the IEEE-603 criteria nor all of the numerous other applicable regulatory guidance, codes, and standards. It is also not intended to provide an exhaustive list of all ITAAC or DAC activities, only those that confirm the aforementioned essential design principles and subjective attribute.

The discussion in this appendix is structured to summarize the key design features of each platform to address the above. Note the following:

- The discussion identifies bracketed key design features (shown as “{“ and “}^{X}” surrounding the feature or design attribute), in which ^{X} numerically denotes each bracketed design feature with one or more superscript numbers that reference the

entry in Table 7DS-1. Table 7DS-1 then cross-references the table entry to the applicable Tier 1 DAC or ITAAC that assures verification.

- Some bracketed items identify analyses to be performed and a report to be generated. While these reports are applicable to that item, they represent only an example of the many technical reports and numerous documents prepared during design development.

- Subsection 14.3.3.4.1 notes that the DI&C ITAAC related to processes and programs are the Tier 1 Section 3.4B ITAAC (Tier 1 Table 3.4 Items 7 through 15). These ITAAC are the DI&C DAC. The identification of specific Tier 1 ITAAC herein is not all inclusive. Instead, it is focused on the DAC of Tier 1, Table 3.4 and the ITAAC of Tier 1, Table 3.4 and Tier 1, Tables 2.2.5, 2.2.7, 2.4.3, and 2.7.5. Table 7DS-1 provides the cross-references of DAC/ITAAC to the DI&C key design features or attributes.

- The FPGA-based RTIS/NMS platform has inherent and distinct design differences from the microprocessor-based ELCS platform. Therefore, the discussion of each is similar but not identical. In addition, much of the noted DAC/ITAAC are applicable to both platforms. However, when DAC/ITAAC is not applicable to a platform, it is identified as such in Table 7DS-1.

- Figures 7DS-1 through 7DS-4 illustrate features of the DI&C design. These figures are derived from Tier 1 Figures 2.2.7b and 3.4b and Tier 2 Figures 7.1-2, 7.2-8 through 7.2-10, 7.9S-1, 7C1, and various Chapter 21 drawings.

7DS.1 Reactor Trip and Isolation System (RTIS) and Safety-Related Neutron Monitoring System (NMS)

7DS.1.1 Redundancy

The RTIS and safety-related NMS implementation in the FPGA platform conforms to the Single Failure Criterion (Clause 5.1) of IEEE-603. To meet this criterion, the redundancy designed into each of these systems is discussed below.

7DS.1.1.1 Reactor Trip and Isolation System

The RTIS implements the majority of the functions of the Reactor Protection System (RPS) and includes the Suppression Pool Temperature Monitor (SPTM) and the Main Steam Isolation Valve (MSIV) functions of the Leak Detection and Isolation System (LDS). {Four redundant, independent divisions of sensors provide input into the four redundant divisions of RTIS. Each division of RTIS includes modules that make up the Digital Trip Functions (DTFs).}[1, 2, 24, 26] Trip decisions from the DTFs are transmitted to each of the four redundant, independent divisions of modules that make up the Trip Logic Functions (TLFs) within RTIS. The signals are transmitted over dedicated, independent optical cables, which also provide electrical isolation. Each divisional TLF determines the trip state based on a two-out-of-four vote. Each divisional TLF sends its voted trip signal state and status information to separate and independent Output Logic Units (OLUs) within its division. The OLU distributes the automatic and manual trip outputs to the solenoid load drivers for reactor trip and MSIV closure.

To permit surveillance testing or maintenance, bypassing of any single division of sensors (i.e., those sensors whose status is part of a two-out-of-four logic) can be accomplished by means of the manually operated bypass. {This Division-of-Sensors Bypass bypasses the divisional DTF and leaves the DTF's output in a non-tripped state. The Division-of-Sensors Bypass is designed to allow only one division to be bypassed at a time. When such bypass is made, all four divisions of two-out-of-four voting logic become two-out-of-three voting logic, a credible failure can occur, and RTIS can still meet the IEEE-603 Single Failure Criterion (Clause 5.1).}[4]

Bypassing a division of trip logic (i.e., taking a logic channel out of service) can be accomplished by means of the Trip-Logic-Output Bypass. When a Trip-Logic-Output Bypass is in effect, the TLF trip output in the bypassed division is inhibited from affecting the output load drivers, maintaining that division's load drivers in an energized state. {Only one divisional TLF can be bypassed by the Trip-Logic-Output Bypass. The two-out-of-four voting logic arrangement of output load drivers for the RPS and MSIV functions effectively becomes two-out-of-three voting logic, a credible failure can occur, and RTIS can still meet the IEEE-603 Single Failure Criterion (Clause 5.1).}[4]

A high level block diagram of the RTIS is shown on Figure 7.1-2.

7DS.1.1.2 Safety-Related Neutron Monitoring System

The safety-related portion of the NMS consists of the Startup Range Neutron Monitor (SRNM), the Local Power Range Monitor (LPRM), and the Average Power Range Monitor (APRM). The Oscillation Power Range Monitor (OPRM) is a functional subsystem of the APRM.

{At low reactor power levels, the SRNM provides all monitoring of neutron flux. Ten SRNM channels are arranged into four divisions such that each of the four RPS divisions receives all of the SRNM input signals from each of the four redundant SRNM divisions. Failure of a single SRNM channel, once bypassed, will not cause a trip to the RPS. Failure of a single SRNM channel will not prevent proper operation of the remaining trip channels in performing their safety functions and satisfying the IEEE-603 Single Failure Criterion (Clause 5.1).}[20, 22, 23]

{For power range neutron flux monitoring, the LPRMs provide data to the APRM and OPRM. LPRM, APRM, and OPRM are provided in each of the four divisions. The LPRM detector sensors are divided into four redundant groups, each group providing local power range signals to its assigned divisional average power range monitor.}[20] Each LPRM detector can be individually bypassed, with a minimum required number of LPRMs in each division. {Each LPRM detector assembly contains four LPRM detectors. Each LPRM detector assembly provides one LPRM input to each of the four independent and redundant APRM and OPRM channels in the same division. LPRM detectors are mapped to divisions to ensure that each APRM and OPRM channel has a representative view of the reactor core.}[20]

{There are four redundant, independent channels of APRM, with each channel providing a trip signal to each of the four RPS divisions. Any two of the four APRM channels that indicate an abnormal condition will initiate a reactor scram through the

RPS two-out-of-four logic. The redundancy criteria are met so that in the event of a single failure under permissible APRM channel bypass conditions, a scram signal will still be generated in the RPS as required. Thus, the IEEE-603 Single Failure Criterion (Clause 5.1) is satisfied.}[20]

{There are four independent and redundant channels of OPRM. The above APRM channel redundancy condition also applies to OPRM channels. Bypassing a division of APRM bypasses the same division of OPRM. The OPRM trip outputs are separate from the APRM trips to RPS and use similar RPS two-out-of-four voting logic as the APRM, satisfying the IEEE-603 Single Failure Criterion (Clause 5.1). The arrangement and assignment of LPRMs provide core regional monitoring by redundant OPRM channels.}[20]

7DS.1.1.3 Power Supply Redundancy

{Power supply redundancy of the RTIS and the safety-related portion of NMS is provided through four redundant, Class 1E, 120 VAC power sources. The power sources provide an uninterruptible supply of electrical power, one to each division. A loss of one power supply will neither inhibit protective action nor cause a scram, satisfying the IEEE-603 Single Failure Criterion (Clause 5.1).}[3, 21, 25]

7DS.1.2 Independence

Each division of RTIS and NMS can accomplish its safety function regardless of the operability or adverse impact of other redundant divisions or other systems. For RTIS and NMS, functional, physical, electrical, and communication independence exists between redundant safety-related divisions, between each safety-related division and other divisions in other safety-related systems, and between safety-related systems and nonsafety-related systems.

Data independence is exhibited in RTIS and NMS in that only votes to trip and status information are provided across divisional boundaries. The data link information is transmitted in packets with a fixed length, fixed content, and predefined format. Failures in the communication links do not adversely affect operation of the divisions receiving malformed, incorrect, or inappropriate data messages.

7DS.1.2.1 Physical and Electrical Independence

{Each of the four divisions of safety-related NMS and RTIS are physically separated from the other redundant divisions. NMS and RTIS comply with the criteria set forth in IEEE-603, Clause 5.6, and follow the guidance of Regulatory Guide 1.75, which endorses IEEE-384.}[3, 21, 25] Class 1E circuits are identified and separated from redundant circuits and non-Class 1E circuits. Qualified electrical isolation devices are provided in the design when an interface exists between redundant Class 1E divisions and between non-Class 1E and Class 1E circuits. Independence and separation of safety-related systems are discussed in further detail in Subsection 8.3.3.6.2.

{Physical and electrical independence of the instrumentation devices of the system is provided by channel independence for sensors exposed to each process variable. Trip logic outputs are separated in the same manner as are the channels. Signals between

redundant RPS divisions are electrically and physically isolated by Class 1E isolators, including fiber optic cables.}[3] Figure 7DS-2 provides a high-level overview of the RTIS safety function communication between redundant divisions.

7DS.1.2.2 Communications Independence

For the FPGA-based systems, the signals from the instrumentation are hardwired to the RTIS and NMS channels. The modules used to construct the RTIS and NMS systems communicate using dedicated communication links internal to the division. Each communication link has its own independent communications buffer.

The communication data links to be provided to systems external to the FPGA-based system use unidirectional fiber optic communication links from each division. The communication links provide only fixed data sets to the nonsafety-related systems, provide 1E to non-1E electrical and functional isolation, and offer no possibility of data transfer from the non-safety to safety equipment during normal operation. The NMS allows non-safety calibration data to be passed only to one division of NMS when that division is out of service as described in Subsection 7DS.1.2.2.2.

The FPGA-based system includes self-diagnostic functions that continuously verify proper FPGA and communications performance, and provide outputs used to alert the operator. If a failure is detected, the division is marked as inoperable (i.e., tripped). When two divisions are in a tripped state, the two-out-of-four voting logic will cause the safety action to occur (e.g., two tripped RPS divisions will scram the reactor). Self-diagnostic functions are safety-related.

Each RTIS and safety-related NMS division has fiber optic communication links to the ELCS communication interface in the same division. The ELCS provides the information for display on the safety displays in the main control room. The links provide a qualified and isolated, point-to-point, single direction communication path to preserve independence between the originating RTIS/NMS division and ELCS.

Each RTIS and safety-related NMS division communicates data and status to the nonsafety-related Plant Information and Control System (PICS) through dedicated communication interfaces in each system's modules. {The communication interface for each division consists of unidirectional fiber optic communication links that broadcast fixed data sets from each safety division to the nonsafety-related PICS. The communication interface is designed to prevent any data transfer from the non-safety PICS to the originating safety related division. The fiber optic cable provides electrical isolation and the safety-related transmitter provides the functional isolation.}[17]

No other capabilities exist for communication with external devices. Communications information specific to RTIS and NMS are discussed briefly below in the following subsections.

7DS.1.2.2.1 Reactor Trip and Isolation System

RTIS includes the primary functions of RPS, and Main Steam Isolation Valve (MSIV) functions of the Leak Detection and Isolation (LDS) subsystem. Each system or

subsystem consists of four redundant divisions. A high level block diagram of one division of the RTIS data communication interfaces is shown in Figure 7.9S-1. Figure 7DS-1 provides a diagram of one RTIS division of trip logic.

{The RPS and MSIV functions are implemented in the four redundant divisions of RTIS. Sensor signals are hardwired to the DTF inputs for each division. Each division's DTF determines the trip status for each signal. The DTF communicates its division's trip status information to the TLF by fiber optic communication links. Because individual divisional trip determinations must be shared between divisions to support two-out-of-four voting logic for divisional trip outputs, the DTF also communicates its trip status information to the other three divisional TLFs by means of isolated fiber optic communication links. The links provide a qualified and isolated, point-to-point, single direction communication path between divisions to preserve divisional independence.}[15, 24]

{Data communicated between RTIS divisions for use in two-out-of-four voting has their own independent communication buffer in the receiving division's TLF for each set of incoming data. Only discrete (vote to trip only) information is transmitted across division boundaries in fixed format, fixed length, and pre-defined messages. This preserves data independence between divisions in accordance with IEEE-603 Clause 5.6.}[7]

The TLF in each division determines the system-level actuation of RPS and MSIV safety functions utilizing two-out-four voting logic. In each division, the TLF communicates trip status information to the OLU by unidirectional fiber optic communication links. The OLU in each division communicates with the Load Drivers that initiate the safety function. {The RPS Load Drivers are hardwired to its scram solenoid valves, and the MSIV Load Drivers are hardwired to its MSIV solenoid valves.}[24, 26]

7DS.1.2.2.2 Safety-Related Neutron Monitoring System

The safety-related NMS consists of LPRM, APRM, and SRNM subsystems, and OPRM, which is a functional subsystem of the APRM. Each subsystem consists of four redundant divisions. There is no communication between redundant divisions in the safety-related NMS. All trip voting is performed in RTIS. A high-level block diagram of one division of the NMS data communication interfaces is shown in Figure 7.9S-1.

The LPRM monitors neutron flux in the power range. {For each of the four NMS divisions, the LPRMs monitor neutron flux levels from the hardwired LPRM detector inputs.}[20] Each division has 52 LPRM detectors and LPRM modules that provide data to the APRM and OPRM in each division. {The LPRM modules in one division communicate internally with the APRM in that division over unidirectional fiber optic communication links, providing fixed data sets of LPRM information.}[15, 20]

For each of the four NMS divisions, the APRM uses the divisional LPRM detectors and a divisional core plate differential pressure input. {When an APRM division detects a trip condition, it provides a hardwired, discrete (vote to trip only) signal to all divisions of the RTIS TLF. The hardwired signals are electrically isolated.}[20]

For each of the four NMS divisions, the divisional OPRM receives local power level data from the divisional LPRMs and core flow and average power level data from the same divisional APRMs over unidirectional fiber optic communication links. {The four divisions of the OPRM trip protection algorithm independently detect thermal hydraulic instability and provide hardwired, discrete (vote to trip only) signals for the RTIS's OPRM voter logic.}[20]

The divisional SRNM monitors neutron flux while in the start-up range. {Each SRNM receives input from a hardwired detector.}[20] SRNM detectors are distributed throughout the reactor core and assigned to four divisions. {Each SRNM detects high neutron flux or a short period condition and provides a hardwired, discrete (vote to trip only) signal to all division of the RTIS TLFs for reactor trip determination.}[20]

The NMS also includes an off-line capability to transfer calibration data from PICS to NMS. When NMS is online and not bypassed, data transfer to NMS from the non-safety system is blocked by a key lock switch in each LPRM module. When calibration information is to be transferred from the nonsafety-related core monitor function of the PICS, the NMS division desired to receive the information must be bypassed by the control room operator, placed in an inoperative status, and the key lock switch on that NMS division must be enabled to request and allow the data transfer. Only a limited data set in a predefined format will be accepted by the NMS. Before the data can be used by the NMS, manual verification and acceptance of each data item at the NMS human-system interface is required. {No online data transmission from nonsafety-related systems to safety-related systems is permitted.}[17]

The Multi-channel Rod Block Monitor (MRBM) is a nonsafety-related subsystem of NMS. {The APRM in each NMS division communicates to the MRBM subsystem with unidirectional fiber optic communication links that provide fixed data sets from each safety division to the nonsafety-related MRBMs.}[15, 17]

7DS.1.3 Determinism

The response time requirement for each NMS and RTIS safety-related function is determined by the Safety Analysis. The response time must be predictable and repeatable to be considered deterministic. The response time for all NMS and RTIS safety functions is deterministic. A description of the FPGA platforms that make the NMS and RTIS response deterministic is provided below.

The FPGA-based system designs use multiple FPGAs on some modules. To enhance testability and reduce undesirable circuit behavior, the basic architecture within each FPGA is a clocked sequential circuit, with periodic synchronizing registers within the FPGAs. Each FPGA only starts processing data when data is transferred into that FPGA, and sends data to the next FPGA or module when processing is complete. Thus, the functions in a given module execute in sequence that is inherently deterministic based on the clocked sequence. The first FPGA completes its function, and then provides data to the next FPGA. When that FPGA completes its function, it provides data to the next FPGA. In addition, when all signal processing FPGAs have finished passing data to the next, the signal processing watchdog timer on the module resets and restarts timing. The watchdog timer is hardware based and is diverse from

the FPGA circuits on each module. {Failure of a signal processing FPGA to complete and pass data to the next FPGA will result in all subsequent FPGAs on that module failing to start. If this occurs in the FPGAs that implement the signal processing and thus the safety functions, the module is marked as failed, the watchdog timer times out, resulting in the tripped division, and an alarm is provided to the operator. Two tripped divisions will result in a reactor scram via the two-out-of-four voting arrangement. The watchdog timer on each module is designed to be fully testable.}[7]

Because FPGAs are arrays of logic cells and registers, each cell connected in series adds defined delay to the logic circuit. {As a result, the logic within each FPGA is designed, verified, and validated to ensure operation within timing constraints under expected operating conditions. The clocked synchronous design is used within each FPGA to avoid timing errors and to ensure timing constraints are satisfied. For synchronous design, changes of state within the FPGA occur only at selected times, controlled by a timing signal. The logic within each FPGA is designed to ensure that the design provides adequate shaping on the inputs to the FPGA to providing sufficient slew on the signal edges.}[8]

{To avoid timing errors within FPGAs, analysis and simulation are performed during the design process. This two-part process includes static timing analysis and dynamic timing simulation. Static timing analysis demonstrates that the setup and hold times on each path within the FPGA design are within predetermined parameters. Software tools used to perform the static timing analysis also are used to evaluate the propagation delay to each element in the code to confirm each timing path in the code is within predetermined paramaters. Also, a diverse set of dynamic simulation software tools are used to validate the design, using predetermined, accurate propagation delays, which are set based on the chosen cells and paths within the routed FPGA. These analyses provide data to the designer to verify that appropriate logic implementation has been achieved, eliminating any potential concerns regarding signal races, signal setup and hold times, and clock skew. A report is generated for implementation including safety analyses.}[10]

{The communication protocols used in the FPGA platforms are deterministic because they are pre-defined, fixed length, fixed format, and generated at specific times in the FPGA logic execution. The communication links that perform safety functions include data and time out error checking to ensure determinism. All detected errors are alarmed. The communication protocols and logic in the communication receivers include self-diagnostics that will generate module failure signals upon detection of communication failures, alerting operators.}[7, 16, 18]

In summary, the FPGA-based, safety-related NMS and RTIS are deterministic. The FPGA platform does not utilize any non-deterministic data communication, non-deterministic computation, interrupts, multitasking, dynamic scheduling, or event driven design. The logic design of the FPGA circuits is fixed and clocked. {The response times for the system elements, including architecture, communications (including timing and loading) and processing elements are tested to verify that the systems' performance characteristics are consistent with the safety requirements established in the design basis for these systems. The analyses are performed to

satisfy the design timing requirements set forth in Clause 4.10 of IEEE-603. A report is generated to demonstrate the adequacy of the timing analysis.}[10]

7DS.1.4 Diversity

The diverse SSLC protection systems allow the overall SSLC safety systems to provide protection against postulated software common cause failures (CCFs). The RTIS and NMS platforms satisfy all IEEE-603 requirements and are developed using a robust hardware/software development process that meets Tier 1 Section 3.4B and BTP 7-14.

The RTIS and NMS are diverse to the Engineered Safety Features (ESF) Logic and Control System (ELCS), which actuates the ESF actions. RTIS and NMS are implemented through FPGA-based platforms, which use configurable logic devices. The ELCS equipment uses microprocessor-based controllers where the logic is implemented in software. The RTIS and NMS are also diverse from the non-safety platforms used for the Nuclear Steam Supply System (NSSS) and Balance of Plant (BOP) control and display.

{The design includes features that enhance the diversity of RPS and MSIV closure functions, including a diverse system for mitigation of Anticipated Transient Without Scram (ATWS) events.

The defense-in-depth configuration for STP 3&4 includes fail-safe RPS systems and fail-as-is ESF systems in separate processing channels. BOP control systems are independent of RPS, NMS, and ELCS in separate communication functions using diverse hardware and software from the Essential Communication Functions (ECFs).}[14]

The STP 3&4 diversity and defense-in-depth strategies are provided in more detail in Tier 1 Section 3.4C and Tier 2 Appendix 7C.

7DS.1.5 Simplicity

The FPGA-based platform that implements safety-related NMS and RTIS is designed for simplicity. The systems have some analog circuits that process detector signals as inputs. The analog signals are converted to digital signals, and then processed by FPGA circuits. The FPGA circuits are constructed of discrete logic blocks that are similar to older, analog and discrete relay circuits in existing operating plants. The FPGA-based DI&C implements the required functionality in fixed gates with deterministic timing that cannot be changed after being programmed at the vendor facility. Priority modules are not necessary due to the simple, overall ABWR diversity strategy. Nonsafety-related equipment is designed such that it cannot control or influence the operation of safety-related functions; nonsafety functions are not performed in the safety-related equipment, which simplifies the safety-related equipment by elimination of non-essential functionality. Data is transferred from each safety division over independent, unidirectional communication links to nonsafety-related equipment for several purposes, including diverse display of safety data, preserving data for historical purposes, and performing channel cross checks. This

transfer of data shifts these complex activities to the non-safety equipment, preserving simplicity in the safety systems. The only communication between divisions is to vote on two-out-of-four trip decisions in RTIS; NMS has no inter-division communication. Thus, the RTIS and NMS platform design satisfies the subjective attribute of simplicity.

7DS.2 Engineered Safety Features Logic and Control System (ELCS)

7DS.2.1 Redundancy

{There are four divisions of sensor functions in ELCS that provide sensor input to the divisional Digital Trip Function (DTF). There are three divisions of system-level safety function initiation in the Safety Logic Function (SLF) and component control in the SLF Remote Digital Logic Controller (SLF RDLC). Divisions I, II, and III contain a DTF sensor division, SLFs for ESF system-level initiations, and SLF RDLCs for component control functions. Division IV contains a DTF sensor division only.}[1, 2]

A Division of Sensors Bypass is provided for surveillance testing and maintenance. {The Division of Sensors Bypass provides independent bypass signals to each division of ELCS. The Division of Sensors Bypass is designed to allow only one division to be bypassed at a time.}[4]

If one of the four divisions of sensors is bypassed, one divisional DTF is bypassed, and three redundant divisions of sensors remain operable. Because the system-level ESF initiation logic is two-out-of-three with a sensor division bypassed, ELCS can experience a credible single failure with a division of sensors bypassed and still meet the IEEE-603 Single Failure Criterion (Clause 5.1).

Each ESF safety function is assigned to a minimum of two divisions. Each of the division's system-level initiation and component level actuation is redundant in at least one other independent division. This assures that the ELCS complies with the IEEE-603 Single Failure Criterion (Clause 5.1).

{There are four 125 VDC redundant power sources, one for each division of ELCS. There are four redundant 120 VAC uninterruptible power sources, one for each division's safety Flat Panel Displays. Because the divisional power sources are independent, the power sources meet the IEEE-603 Single Failure Criterion (Clause 5.1).}[3]

7DS.2.2 Independence

A division of ELCS will accomplish its safety functions regardless of the operation or failure of other safety divisions, or the operation or failure of non-safety systems. A high level block diagram of one division of the ELCS data communication interfaces is shown in Figure 7.9S-1. Figure 7DS-3 provides a diagram of one ELCS division of ESF safety function initiation and component actuation.

{There are four divisions of sensor functions in ELCS that provide sensor input to the divisional DTF. There are three divisions of system-level safety function initiation in the SLF and component control in the SLF RDLC. Divisions I, II, and III contain a DTF, SLFs for ESF system-level initiations, and SLF RDLCs for component control

functions. Division IV contains a DTF sensor division only.}[1, 2] {ELCS equipment is Class 1E.}[1] {The ELCS software is safety-related and is developed in compliance with Tier 1 Section 3.4B and BTP 7-14 to conform to the requirements for service in a Class 1E application.}[5, 8, 11, 12, 13] The ELCS description of Independence includes these topics:

- Functional Independence
- Physical Independence
- Electrical Independence
- Communications independence

These topics are discussed individually in the following subsections.

7DS.2.2.1 Sensor DTF Division Functional Independence

{Each division of ELCS has independent sensors. There are no shared sensors between divisions of DTFs. There is no communication between ELCS DTFs in independent divisions. This assures that the input data for each division is independent.}[1, 3 ,15]

Each ELCS sensor division operates asynchronously from the other divisions. Each sensor division performs its safety function independently from the other sensor divisions. {Each sensor division DTF independently transmits the ESF safety function initiation information as a discrete value (vote to initiate only) to the three divisions of system-level initiation logic and component control.}[3, 15]

Each sensor division transmits the division's DTF initiation status over a unidirectional point-to-point serial data link. There is no interaction between the transmitting sensor division and the receiving division as described in Subsection 7DS.2.2.4.1.

{Where an external system needs direct sensor information from ELCS for display or recording, the ELCS analog or digital signal is isolated by a qualified isolation device before the signal enters the ELCS data acquisition equipment.}[1, 3, 17] Thus, no failure in the external system can adversely affect the direct sensor information in ELCS.

{Each external discrete signal that is hard wired to a division of ELCS is isolated by a qualified isolation device to assure that the independence of the ELCS division is maintained. The qualified isolation device is Class 1E ELCS equipment.}[1, 3, 10, 15]

7DS.2.2.2 Physical Independence

{Each of the four divisions of ELCS is physically separate from the other redundant divisions.}[3] The ELCS enclosures and equipment are seismically qualified to assure that a seismic design basis event cannot compromise the physical separation.

{All of the ELCS divisions are physically separated from the non-safety systems.}[3]

7DS.2.2.3 Electrical Independence

7DS.2.2.3.1 Independent Power Sources

{Each redundant division is powered by separate independent divisional power sources. Each division's sensors, DTF, SLFs, and SLF RDLCs receive their power from a separate and independent divisional Class 1E 125 VDC power source.}[3, 19] {The ELCS safety Flat Panel Displays in each division is powered from a separate and independent divisional source, which is the 120 VAC uninterruptible Class 1E power supply.}[19]

{The ELCS power sources are independent and separate from the non-safety power sources.}[3, 19]

7DS.2.2.3.2 Electrical Isolation

{Each ELCS division is electrically isolated from the other redundant divisions.}[3] {Each DTF transmits the division's ESF safety function initiation status over a point-to-point fiber optic cable to each SLF in the three independent divisions. Because the communication is unidirectional, isolated, and buffered, from the DTF to the SLF, there is no possibility of interaction between the transmitting DTF and the receiving SLFs that would propagate an electrical fault or degrade the independence of the sending division from the receiving division.}[1, 17]

Each SLF transmits ESF safety function system-level initiation status to Remote Digital Logic Controllers (RDLCs) in the same division as the SLF over redundant, point-to-point, fiber optic, serial data links. Because the transmission is unidirectional, isolated, and buffered, there is no possibility of interaction between the transmitting SLF and the receiving SLF RDLCs. {Because the fiber optic link from the DTF RDLC is redundant, the communication can accommodate a single cable break or failure of a fiber optic modem and continue to function without interruption.}[18] The RDLC performs the component control logic and provides control commands to a Component Interface Module (CIM), which provides the resultant control signals to the electromechanical component. The CIM provides qualified isolation for the component feedback signals.

Figure 7DS-4 provides a high level overview of the ESF safety function communication between redundant divisions.

The Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring System (NMS) provide serial, unidirectional communication interfaces to ELCS to provide the capability for ELCS to display RTIS and NMS information. Communication from RTIS and NMS to ELCS remains within the same electrical division. These communication interfaces utilize fiber optic isolation. ELCS provides communication buffering in the communication interface to the safety Flat Panel Displays.

{Each ELCS division is electrically isolated from the non-safety systems.}[3] {Each ELCS division has a single unidirectional, fiber optically isolated communication link to the non-safety system. Both the communication protocol and the transmission

interface are designed such that it is not possible for the non-safety system to send data to ELCS over this communication link.}[17]

{Each external discrete signal that is hard wired to a division of ELCS is isolated by a qualified isolation device to assure that the independence of the ELCS division is maintained. The qualified isolation device is Class 1E ELCS equipment.}[1, 3, 10, 15]

These measures assure the electrical isolation and independence of each ELCS division.

7DS.2.2.4 Communications Independence

There are three types of data communication utilized for ELCS. These types are:

- Unidirectional serial point-to-point fiber optic data link
- Intra-division network
- Safety to Non-safety

7DS.2.2.4.1 Unidirectional Serial Point-to-Point Fiber Optic Isolated Data Links

{The unidirectional serial point-to-point fiber optic isolated data link utilizes a deterministic protocol.}[16] Each transmission is unidirectional from the transmitting controller to the receiving controller. The communications occur in a predictable, cyclic sequence. The communication is buffered by the communication processor, which is separate from the application processor on both the sending and receiving end of the communication process. {The unidirectional nature of the communication process in conjunction with the buffering of the communication from the application processor and the electrical isolation complies with the independence requirements of IEEE 7.4.3-2.}[7, 19]

This type of communication link is utilized to communicate automatic and manual ESF safety function information. The link is utilized to communicate ESF safety function information within a division including:

- DTF RDLC to DTF in the same division
- DTF to SLFs in the same division
- SLFs to RDLCs in the same division

This type of communication link, using separate communication equipment, is also used between divisions from a division's DTF to the SLFs in the other divisions.

{This assures that there are no communication interactions that would affect the independence of the divisions.}[19]

Unidirectional Data Communications Functions for ELCS

{Each division's DTF RDLC transmits converted sensor signals to the division's DTF. The DTF RDLC transmits the signal information to the DTF by redundant, isolated, unidirectional, point-to-point, serial data links. The links are isolated by fiber optic media. This communication is sent without requiring an acknowledgement from the receiving DTF.}[1]

The DTF receives the transmission and then determines the division's ESF safety function initiation status. The DTF then uses separate unidirectional, point-to-point, serial links to transmit the division ESF safety function initiation status as discrete data containing only the votes to initiate protective action, to each duplicate SLF in each division. These links are isolated by fiber optic media. Each of these SLFs receives an isolated unidirectional serial link from the DTF in each division. {The SLF utilizes the four sets of independent DTF ESF safety function initiation status data and determines if there is a coincidence of two initiation signals for a specific safety function. The SLF then transmits the system-level initiation status over a redundant, isolated, unidirectional serial link to the SLF RDLCs. The links are isolated by fiber optic media. The SLF RDLC receives the system-level initiation status and provides the appropriate component actuation control command to the Component Interface Module (CIM).}[1]

Component Interface Module (CIM)

{The CIM is implemented with non-microprocessor technology. A CIM is assigned to each plant component controlled by ELCS. The CIM provides the hard wired interface to the component control circuit and receives the hard wired feedback signal from the component that provides component status information.

A CIM will receive input control commands from two SLF RDLCs for components where it is desired to reduce the probability of spurious actuation. For this case, the CIM performs 2-out-of-2 coincidence logic for the commands received from two SLF RDLCs. The capability exists to bypass an ESF output channel for maintenance or surveillance testing. When an ESF output channel is bypassed, the CIM reverts to a 1-out-1 logic that utilizes the output channel that is not bypassed.}[1, 2, 4] For ESF functions that utilize a single SLF RDLC, the CIM uses 1-out-of-1 logic. The CIM communicates the component status feedback information to each SLF RDLC that provides output commands to it.

{The use of the communication methods described above for the ESF safety function automatic and manual initiation assures that the divisions are independent.}[3] Data independence is maintained by this communication method. The SLF is the only point where multiple sets of independent data are processed. {The SLF has a different receive port for each of the four independent DTF data sets. The SLF uses the independent discrete data sets in coincidence logic in a manner that assures that there is no interaction that would degrade the independence of the division.}[7, 15, 17] A description of the use of the independent data sets is provided in Subsection 7DS.2.3.3.

{Messages are sent and processed in a pre-determined format, with known lengths and data mapping within the messages. Any message that does not match the requirements provided in the communication protocol will be discarded. Only correctly formatted messages can be used. The predefined formatting and data redundancy within the message minimize the possibility of malformed messages from being used by the receiving Controller's application processor.}[1]

The design of the controller utilized for communication assures that the Boolean data communicated for the ESF safety function status cannot be used as a controller instruction. Information on this topic is provided in Subsection 7DS.2.3.3.

7DS.2.2.4.2 Intra-division Network Communication

{Each ELCS division includes an intra-division network for communication within the division. This network is separate from the ESF safety function communication. The intra-division network uses a deterministic protocol.}[16]

The intra-division network uses a communication interface module to buffer communication data from each application processor. The communication interface module receives data from the application processor in buffered memory and the communication interface module writes data to the buffered memory for the application processor to read. This assures that the application processor will perform deterministically, independent of the intra-division network status. The communication interface module performs the network communication function and diagnostics on the messages received. {The intra-division network utilizes redundant fiber optic isolating media between ELCS cabinets in separate locations such that the intra-division network can accommodate a single failure of a fiber optic modem or a single cable break and continue to function.}[7]

The intra-division network provides the following functions:

- Provides signal information and component status to the safety Flat Panel Displays. The Flat Panel Displays are dedicated to a division. {There is no capability to transmit or receive information from an external division or non-safety system from a division's safety Main Control Room Flat Panel Displays.}[17, 19]

- {Provides the capability for operator soft control for selected division components by means of the plant operators' safety Flat Panel Displays in the Main Control Room. There is no functionality or communication capability that would allow a division's safety Flat Panel Display to control components in another division.}[15, 18]

- {Provides the capability to communicate self-diagnostic information for display and alarm in the Main Control Room.}[15]

- Provides the capability for maintenance display of detailed diagnostic information and the capability to conduct surveillance testing at the Maintenance and Test Panel (MTP) installed in each division. {The MTP does not have the ability to control components in a division or communicate across divisions.}[1]

{The loss of the intra-division network will not affect the division's ability to perform the manual and automatic ESF safety function initiation and component actuation. The intra-division network does not extend beyond a division's boundary. The intra-division network has no interfaces with nonsafety-related systems. Therefore, the intra-division network adheres to the design principle of division independence.}[17, 19]

7DS.2.2.4.3 Safety to Non-Safety Communication

{Each independent ELCS division has a communications interface to the Plant Information and Control System (PICS). The ELCS Maintenance and Test Panel (MTP) provides buffered, unidirectional communications over a fiber optically isolated interface. The MTP buffers the data that is received from the intra-division network. The MTP utilizes a separate communication interface to transmit a subset of the buffered data to PICS. The MTP communication interface does not have the capability to read data. Data is transmitted without acknowledgement to the non-safety system.}[15]

7DS.2.3 Determinism

7DS.2.3.1 Overview

The response time requirements for ELCS are determined by the Safety Analysis for each ESF safety function. The ELCS response time must have a predictable and repeatable maximum value that meets the Safety Analysis requirements under all plant operational conditions determined by the STP 3 & 4 design bases.

If the response time is predictable and repeatable, then it is deterministic. The ELCS response time for all ESF safety functions is deterministic. {A formal timing analysis is developed to document the response time and meets the requirements of Clause 4.10 of IEEE-603. The analysis is validated by formal test. A report is generated to demonstrate the adequacy of this timing analysis.}[9]

A description of the ELCS design features is provided in this section. These design features assure that the design is deterministic and that the response time meets the Safety Analysis requirements for each ESF safety function.

7DS.2.3.2 Signal Input

The signal inputs represent the state of plant processes that indicate the need for an ESF safety function initiation. The sensor response time and the analog filtering of the signal determine the delay time before a signal level reaches the setpoint where an ESF safety function is required to be initiated. This delay time is included in the above timing analysis.

7DS.2.3.2.1 Signal Measurement

The signal inputs are converted to internal digital values by the analog input modules and digital input modules. The data acquisition modules function independently from the controller application processor and contain buffered values that are available for

the processor to read. The maximum delay time from signal measurement to the availability of the data to be read is included in the above timing analysis.

7DS.2.3.2.2 ELCS Controller Processing

The ELCS controller consists of an application processor and a communication processor. The two controller processors are separate and each contains its own local memory. The two separate processors share a distinct portion of memory where the information is stored for unidirectional point-to-point serial links communication. Each separate datum has a unique shared memory location. The location of the data sent by the application processor is separate from the location where the data received from the communication processor is stored. The application processor is buffered from the communication processor by shared memory so that the application processor timing is not affected by communication with other controllers.

The application processor is also buffered from the intra-division network by different buffered memory for transfer to the intra-division network communications interface module.

Communications Processor for Unidirectional Serial Communication

ELCS is designed such that all information required for ESF safety function initiation is communicated every time the communication occurs. There is no data that is communicated by “exception.”

The communications processor supports the deterministic performance of the unidirectional serial data link communications. The communication processor performs the following functions:

- Receives and buffers incoming data from each unidirectional serial link. Each unidirectional serial data message has a predetermined size that cannot exceed a predetermined maximum size.
- Provides communication diagnostics on the incoming communication message
- Formats the incoming data and stores the data in predetermined locations in memory that is shared by the application processor
- Reads the outgoing communication data from the memory shared by the application processor
- Formats the data into one outgoing message, including additional data for diagnostic purposes and provides a CRC data for the message.
- Transmits the outgoing message

The communications processor is designed to provide sufficient spare capacity such that there is a maximum fixed delay time to perform each function. The input communications are sent by a cyclic deterministic process from the transmitting processors. The output communications are initiated by the cyclic, deterministic

application processor application software modules. Because the input data is cyclic and predictable and the output data is cyclic and predictable, the communications processor performs deterministically, within the requirements of the Safety Analysis.

The applications processor performs the following functions for an application software module:

- Reads the input signals from the data acquisition modules
- Reads the unidirectional serial communication data from the memory shared by the communications processor
- Reads the communication data from the buffered memory for the communication interface module for the intra-division network
- Performs the ESF safety function algorithm calculations and logic
- Writes output signals to discrete output data modules (if the applications process has output data modules)
- Writes the output data to shared memory in the communication processor for the unidirectional serial link
- Writes the output data to buffered memory for transfer to the communications interface module for the intra-division network

The time for each of these steps has a fixed maximum delay that can be determined based on the fixed amount of data input and data output and the maximum computation time for the calculations and logic. These delay times are used to determine the minimum cycle time for application software module scheduling. Additional time margin is added to the minimum cycle time to determine the design cycle time for the application software module execution.

The scheduling of the execution of the application software modules is based on an internal clock with a precision interval timer. The scheduling is fixed by the design. There are no application processor interrupts that are driven by external process signals.

The scheduling of an application software module in an application processor is designed with sufficient margin to allow the program to execute at its predetermined frequency, with sufficient additional time available to assure the internal self-diagnostics have sufficient time to execute. The required time margin is a fixed value that is predetermined. The application processor has a self diagnostic that monitors the execution of the application software modules.

The response time analysis assumes that the input information that would result in an ESF safety function output occurs just after the program is scheduled for execution. This results in a maximum delay time that is equal to the amount of time before the application software module is scheduled to execute again, plus the time that the

program takes to execute and provide its output results. This amount of time is used as the maximum delay time in the above timing analysis.

The overall response time for an ESF safety function includes the delay time for each element in the processing chain from the sensor to the component actuation. This chain of events includes:

(1) Sensor and signal processing delay to the DTF RDLC data acquisition

(2) Signal data acquisition delay

(3) Application software execution delay as calculated above for the DTF RDLC

(4) Communications delay for the unidirectional serial link from the DTF RDLC communications processor to the DTF communications processor

(5) Communications delay from the DTF communications processor to the DTF applications processor and the parallel delay for DTF local data acquisition

(6) DTF application software module execution delay, which is calculated as described above

(7) Communications delay for the unidirectional serial link from the DTF communications processor to the SLF communications processor

(8) Communications delay from the SLF communications processor to the SLF applications processor and the parallel delay for SLF local data acquisition

(9) SLF application software module execution delay, which is calculated as described above

(10) Communications delay for the unidirectional serial link from the SLF communications processor to the SLF RDLC communications processor

(11) Communications delay from the SLF RDLC communications processor to the SLF RDLC applications processor and the parallel delay for SLF RDLC local data acquisition

(12) SLF RDLC application software module execution delay, which is calculated as described above

(13) Communications delay for the unidirectional serial link from the SLF RDLC communications processor to the CIM

(14) Processing delay of the CIM

(15) Time required for the actuated electromechanical component to achieve its predefined actuation state or condition.

{Each step in the process is predictable and repeatable. This is the time response that is designed to meet the Safety Analysis requirements.}[16]

{The timing described above assumes that the signals that require an ESF safety function response occur just after the programs are scheduled to execute. A best case analysis is also determined to establish the shortest response time that could occur if the signal value reached the ESF safety function initiation setpoint earlier. The two response times that are determined in the response time analysis are used to set the criteria for the response time validation test. A report is generated to demonstrate the adequacy of the response time analysis.}[2, 6, 7, 9, 10]

The timing analysis is performed as required by the NRC in the Plant Specific Action Items described in the Safety Evaluation report for the Common Q Topical Report, WCAP-16097-P-A. This topical report provides additional information on the deterministic performance of safety systems based on use of the Common Q platform.

7DS.2.3.3 Inter-division Communications

{Each division's DTF communicates its ESF safety function actuation status to redundant SLFs in its own division and to each of the redundant SLFs in other redundant divisions over point-to-point, unidirectional serial communications data links. Each data link uses fiber optic cable to provide the required electrical isolation between divisions.}[1]

{Each division receives a point-to-point serial data link from four redundant DTFs. The data that is transmitted by each DTF is a Boolean number where each bit in the number defines the DTF initiation status of an ESF safety function. The complete Boolean number contains the complete set of bits for all the ESF safety functions. The SLF communications processor performs a cyclic redundancy check and data redundancy check on the message. A message that passes these self-diagnostics is stored in the predetermined memory locations shared by the application processor. If the self-diagnostics detects a problem with the message, the communication processor sets an error status bit. When the error status bit is set, the application processor uses a predefined value based on the desired failure state. When the message passes the self-diagnostics, the application processor uses the data to perform Boolean logic operations to determine if two or more of the redundant logical data sets include a coincidence of two states that require a system-level initiation of one or more of the ESF system-level safety function initiations.}[1]

There are six coincidence logic sets: (1) DTF A and DTF B, (2) DTF A and DTF C, (3) DTF A and DTF D, (4) DTF B and DTF C, (5) DTF B and DTF D, and (6) DTF C and DTF D.

A single corrupted set of DTF data would only affect the accuracy of three of the six coincidence logic calculations, leaving three valid coincidence logic sets that would provide a valid system-level initiation when required. Even if one of the divisions was in division of sensor bypass, there would still be a valid calculation that would result in a valid system-level initiation when required.

Because the calculations are Boolean logic, the use of a single set of corrupted DTF data in the calculation would only produce an inaccurate result for the calculations that use the corrupted data. This will not prevent the valid data from initiating a valid ESF safety function when required.

If a single SLF failure occurs that results in no initiation output when an initiation is required, then the CIM logic for this case would prevent the ESF safety function initiation in the division that experienced the failure. The redundant set of SLFs in a redundant division would then initiate the system-level ESF safety function initiation, satisfying the single failure criterion by division redundancy.

7DS.2.3.4 Intra-division Communications

The intra-division network is utilized to:

- Communicate signal and component status information to the divisional safety Flat Panel Displays in the Main Control Room and the divisional Maintenance and Test Panel
- Provide the capability for the plant operators to utilize the Main Control Room Flat Panel Displays to control individual components in that division
- Provide the capability for maintenance and surveillance testing from the divisional safety Flat Panel Display at the Maintenance and Test Panel (MTP)

The intra-division network utilizes a communication interface module in the controller chassis. The communication interface module uses buffered memory for each controller chassis on the network to send or receive intra-division network information. The application processor writes the information it needs to transmit on the intra-division network to the buffered memory, and the communication interface module handles the transmission. The intra-division network utilizes redundant fiber optic modems and fiber optic cable for all external connections from one ELCS cabinet to another ELCS cabinet in a different location. The intra-division network utilizes a bus master that controls the network communication to assure that it is deterministic. If the bus master fails, network control automatically passes to the back-up bus master. The bus master and the intra-division communication interface modules provide self-diagnostics to assure that failures are annunciated.

{A timing analysis is performed for the intra-division network to verify meeting the response time requirements for the intra-division network, which were derived from human factors engineering (HFE) considerations.}[1, 2] This timing analysis is required by the NRC's SER for the Common Q Topical Report.

7DS.2.3.5 Self-Diagnostics for Deterministic Performance

7DS.2.3.5.1 Controller

{The applications processor and communications processor in a controller are monitored by a watchdog timer. If the cyclic processing is disturbed by a failure, the

watchdog timer will time-out and cause an annunciation.}[1] In general, each controller has a redundant counterpart that monitors the controller's watchdog timer to alarm this condition.

7DS.2.3.5.2 Unidirectional Serial Communications

The receiving Controller for each unidirectional message monitors the cyclic operation of the communication transmission. {If a new message is not received within a predetermined time interval, the receiver will cause an alarm indicating that the unidirectional serial link has failed and set the value of the message from the failed link to a predetermined value. The receiver also performs a number of diagnostic checks on the transmitted message. If the diagnostic detects a problem with the message, it will set an error status bit. When the error status bit is set, the application processor will use a predefined value based on the predetermined failure state and will alarm the condition.}[18]

7DS.2.3.5.3 Intra-division Network Communications

The bus master monitors the deterministic operation of the network. {Each communication interface module provides diagnostic checks on received messages. The communication interface module will flag bad data so that the application processor can process it in a predetermined manner.}[18]

7DS.2.3.6 Summary of Determinism

The ELCS design features and self-diagnostics assure that the ELCS will perform in a deterministic manner. {Timing analyses are performed to document the deterministic performance. Validation testing is performed to verify that ELCS meets the required response time for ESF safety function actuation. Validation testing is also performed to verify that HFE response time requirements are met. Reports are generated as previously discussed above in this section to demonstrate the adequacy of timing analyses and testing.}[16]

7DS.2.4 Diversity

7DS.2.4.1 Platform Diversity

The ELCS platform is diverse from the equipment that implements the RTIS and NMS. ELCS utilizes a microprocessor-based controller, proprietary protocol for the unidirectional serial communications utilized for the ESF safety functions, and a different proprietary protocol for the intra-division network. The RTIS and NMS utilize FPGA technology and communications protocols that are different from those used by ELCS.

ELCS is also diverse from the non-safety platforms used for NSSS and BOP control and display. ELCS utilizes a different microprocessor and communications protocols.

{ELCS is diverse from the equipment required to mitigate an ELCS failure, as described in Tier 1 Section 3.4C and Tier 2 Appendix 7C.}[14]

7DS.2.4.2 Functional Diversity by Functional Segmentation of SLFs

ELCS is designed with functional segmentation of sets of ESF safety functions. The different sets of ESF safety functions are assigned to different SLFs in each division.

7DS.2.5 Simplicity

7DS.2.5.1 Simplicity of Communications

ELCS uses unidirectional point-to-point data links to communicate automatic and manual ESF safety function initiation information. The use of this method of communication is easily implemented and analyzed to assure deterministic performance.

7DS.2.5.2 Minimization of Communication Between Safety Divisions

ELCS utilizes digital communication between divisions only for the coincidence logic voting function. This simplifies the communication design and simplifies the analysis and validation testing necessary to demonstrate independence.

7DS.2.5.3 Separation of Protection and Control

ELCS does not include non-safety system digital communication control of safety components with priority modules. ELCS control functions originate within each independent division, including dedicated Safety Flat Panel Displays in the Main Control Room.

Table 7DS-1 Cross Reference of the Tier 1 DAC/ITAAC Required for DI&C Verification

DAC/ITAAC Verification	Note	Appendix 7DS RTIS/NMS Subsection Reference*	Appendix 7DS ELCS Subsection Reference*
Tier 1, Table 3.4, ITAAC No. 1	1	1.1.1	2.1; 2.2; 2.2.1; 2.2.3.2; 2.2.4.1; 2.2.4.2; 2.3.3; 2.3.4; 2.3.5.1
Tier 1, Table 3.4, ITAAC No. 2	2	1.1.1	2.1; 2.2; 2.2.4.1; 2.3.2.2; 2.3.4
Tier 1, Table 3.4, ITAAC No. 3	3	1.1.3; 1.2.1	2.1; 2.2.1; 2.2.2; 2.2.3.1; 2.2.3.2; 2.2.4.1
Tier 1, Table 3.4, ITAAC No. 4	4	1.1.1	2.1; 2.2.4.1
Tier 1, Table 3.4, DAC No. 8	5	Coverage in Notes 7, 8, and 10	2.2
Tier 1, Table 3.4, DAC No. 8b & 11	6	†	2.3.2.2
Tier 1, Table 3.4, DAC No. 8e & 11	7	1.2.2.1; 1.3	2.2.4.1; 2.2.4.2; 2.3.2.2
Tier 1, Table 3.4, DAC No. 8g & 11	8	1.3	2.2
Tier 1, Table 3.4, DAC No. 8h & 11	9	†	2.3.1; 2.3.2.2
Tier 1, Table 3.4, DAC No. 8i & 11	10	1.3	2.2.1; 2.2.3.2; 2.3.2.2
Tier 1, Table 3.4, DAC No. 9	11	†	2.2
Tier 1, Table 3.4, DAC No. 10	12	†	2.2
Tier 1, Table 3.4, DAC No. 11	13	Coverage in Notes 7, 8, and 10	2.2
Tier 1, Table 3.4, ITAAC No. 16	14	1.4	2.4.1
Tier 1, Table 2.7.5, ITAAC No. 1	15	1.2.2.1; 1.2.2.2	2.2.1; 2.2.3.2; 2.2.4.1; 2.2.4.2; 2.2.4.3
Tier 1, Table 2.7.5, ITAAC No. 2	16	1.3	2.2.4.1; 2.2.4.2; 2.3.2.2; 2.3.6
Tier 1, Table 2.7.5, ITAAC No. 3	17	1.2.2; 1.2.2.1; 1.2.2.2	2.2.1; 2.2.3.2; 2.2.4.1; 2.2.4.2
Tier 1, Table 2.7.5, ITAAC No. 4	18	1.3	2.2.3.2; 2.2.4.2; 2.3.5.2; 2.3.5.3
Tier 1, Table 2.7.5, ITAAC No. 6	19	†	2.2.3.1; 2.2.4.1; 2.2.4.2
Tier 1, Table 2.2.5, ITAAC No. 1	20	1.1.2; 1.2.2.2	†
Tier 1, Table 2.2.5, ITAAC No. 4	21	1.1.3; 1.2.1	†
Tier 1, Table 2.2.5, ITAAC No. 8	22	1.1.2	†
Tier 1, Table 2.2.5, ITAAC No. 9	23	1.1.2	†
Tier 1, Table 2.2.7, ITAAC No. 1	24	1.1.1; 1.2.2.1	†
Tier 1, Table 2.2.7, ITAAC No. 7	25	1.1.3; 1.2.1	†
Tier 1, Table 2.4.3, ITAAC No. 1	26	1.1.1; 1.2.2.1	†

* All Subsections are preceded by 7DS.

† A particular DAC or ITAAC is not applicable to a system or no verification statements in Appendix 7DS are relevant.

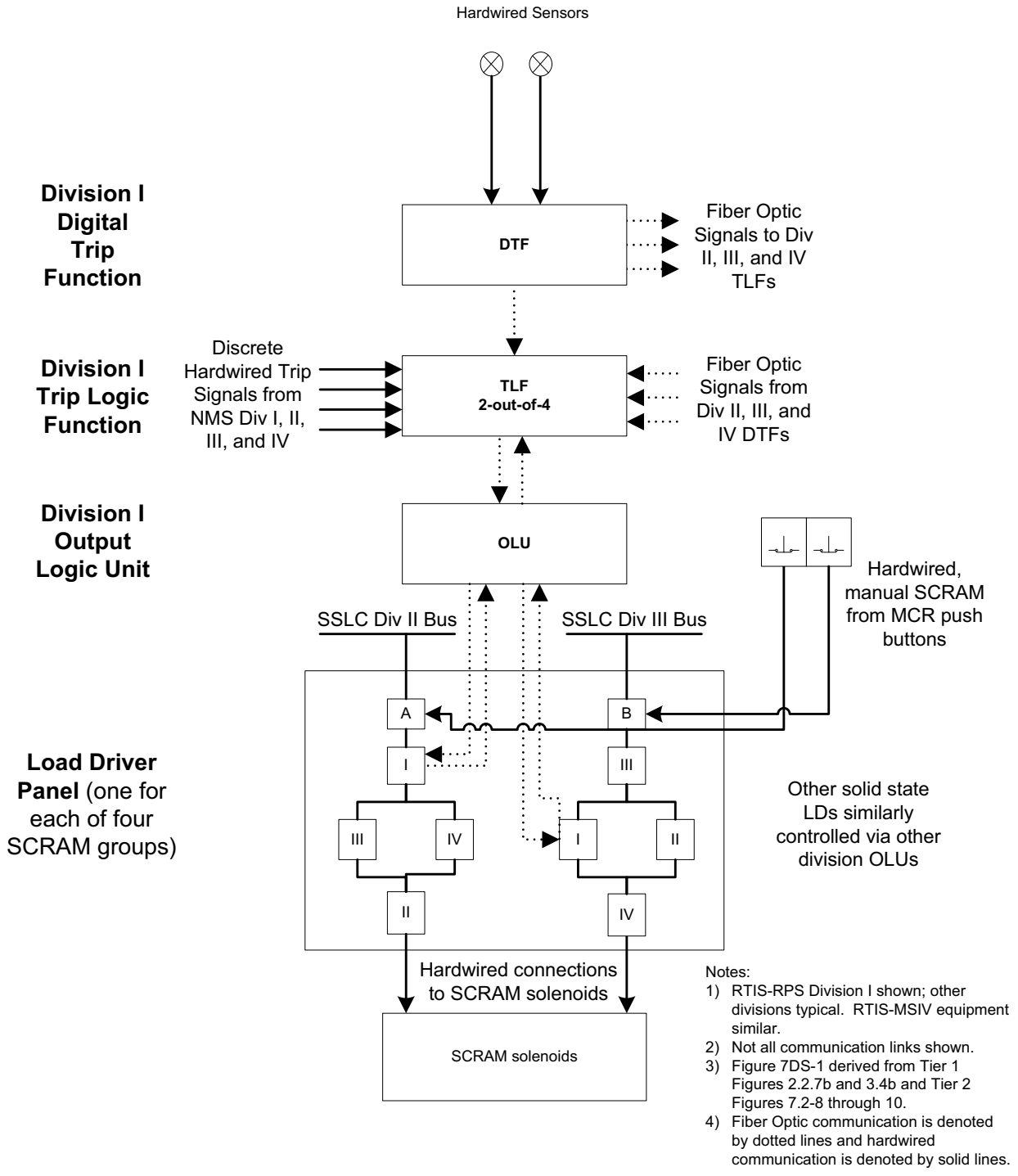
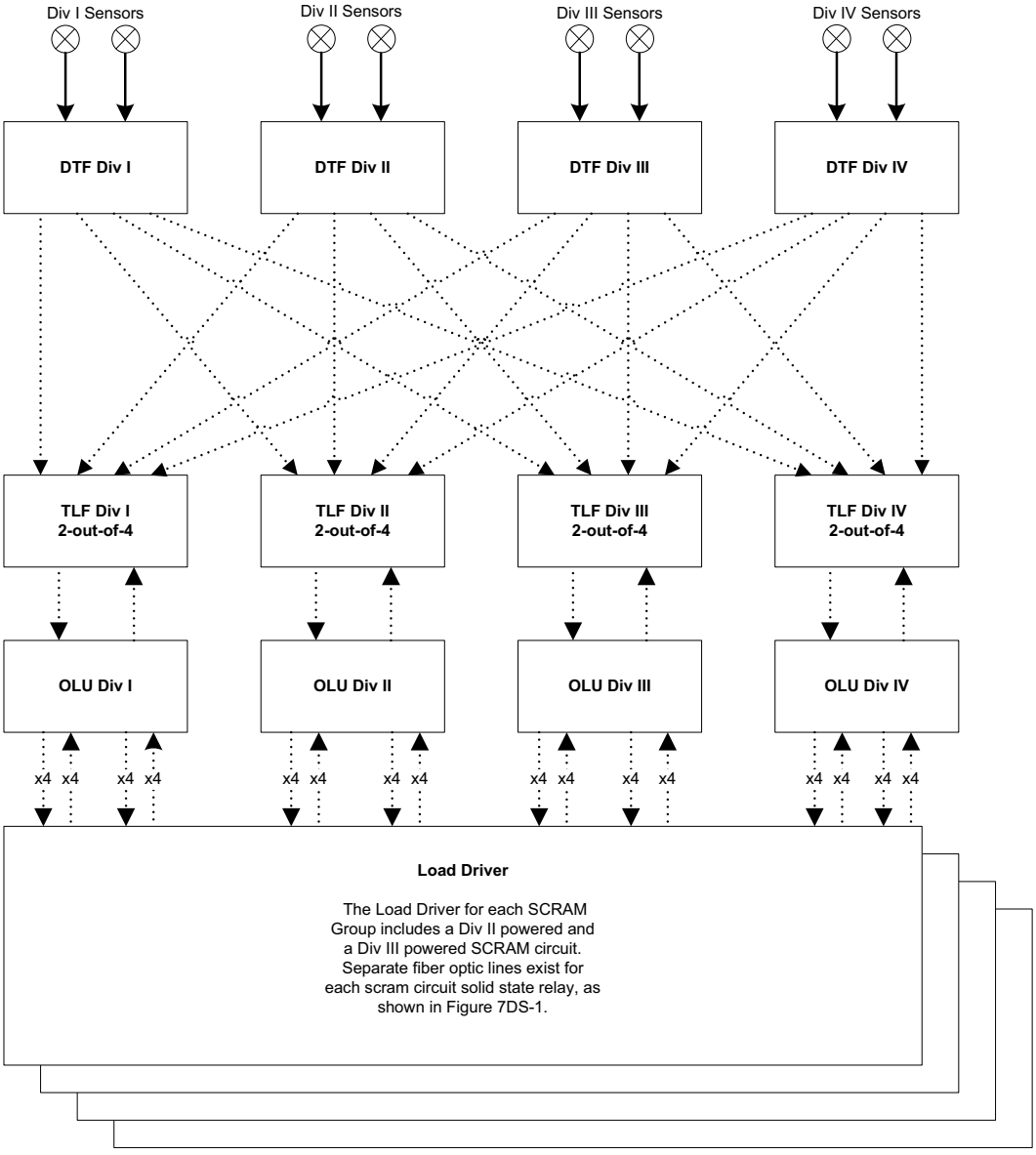


Figure 7DS-1 RTIS Divisional Simplified Block Diagram



Notes:
1) RTIS-RPS Division I shown; other divisions typical. RTIS-MSIV equipment similar.
2) Not all communication links shown.
3) Figure 7DS-2 derived from Tier 1 Figures 2.2.7b and 3.4b and Tier 2 Figures 7.2-9 and 10.
4) Scram solenoids not shown. Hardwired connections to Scram solenoids.
5) Fiber Optic communication is denoted by dotted lines and hardwired communication is denoted by solid lines.

Table 7DS-2 RTIS Inter-division Communication Simplified Block Diagram

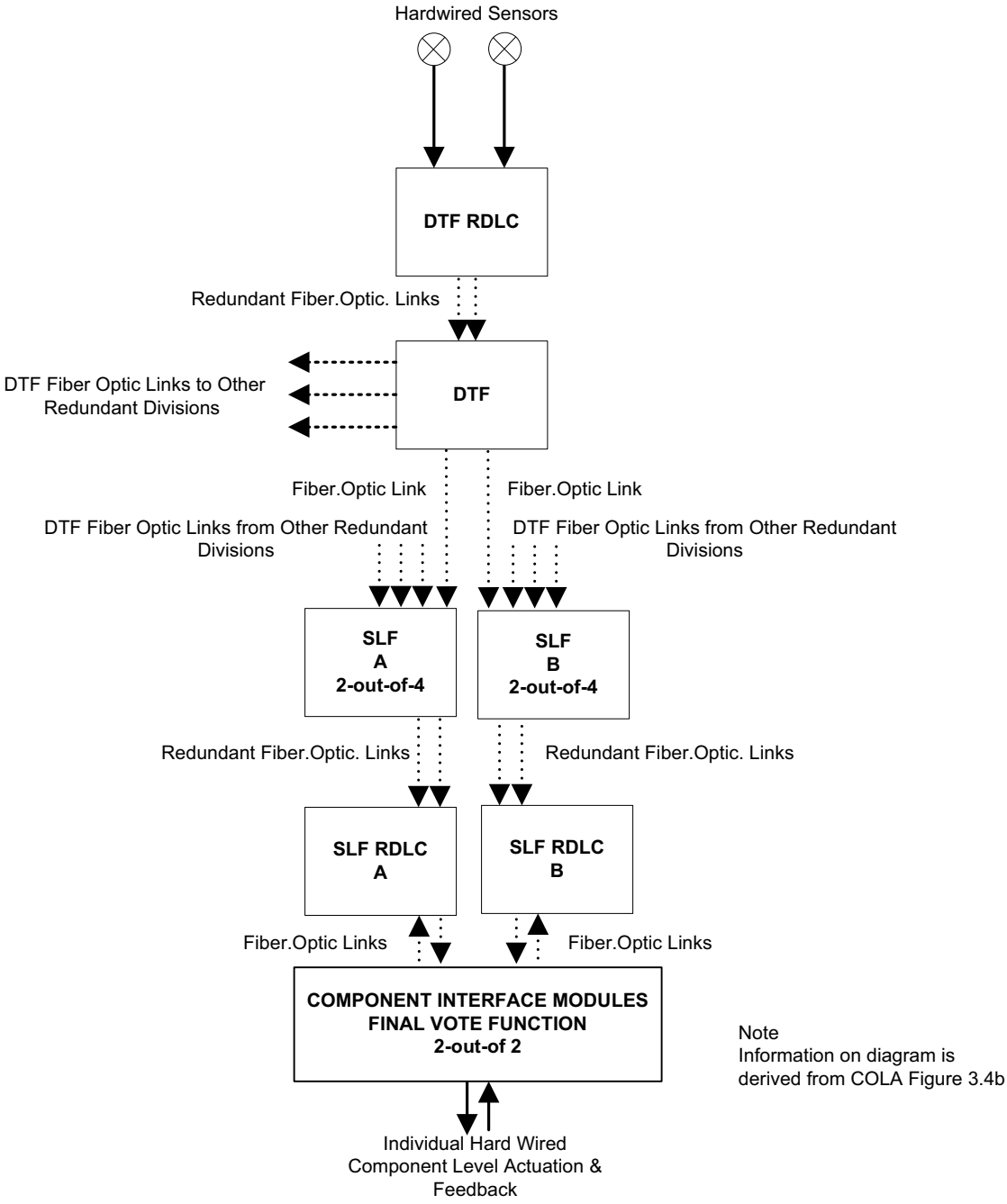


Table 7DS-3 ELCS Single Division Simplified Block Diagram

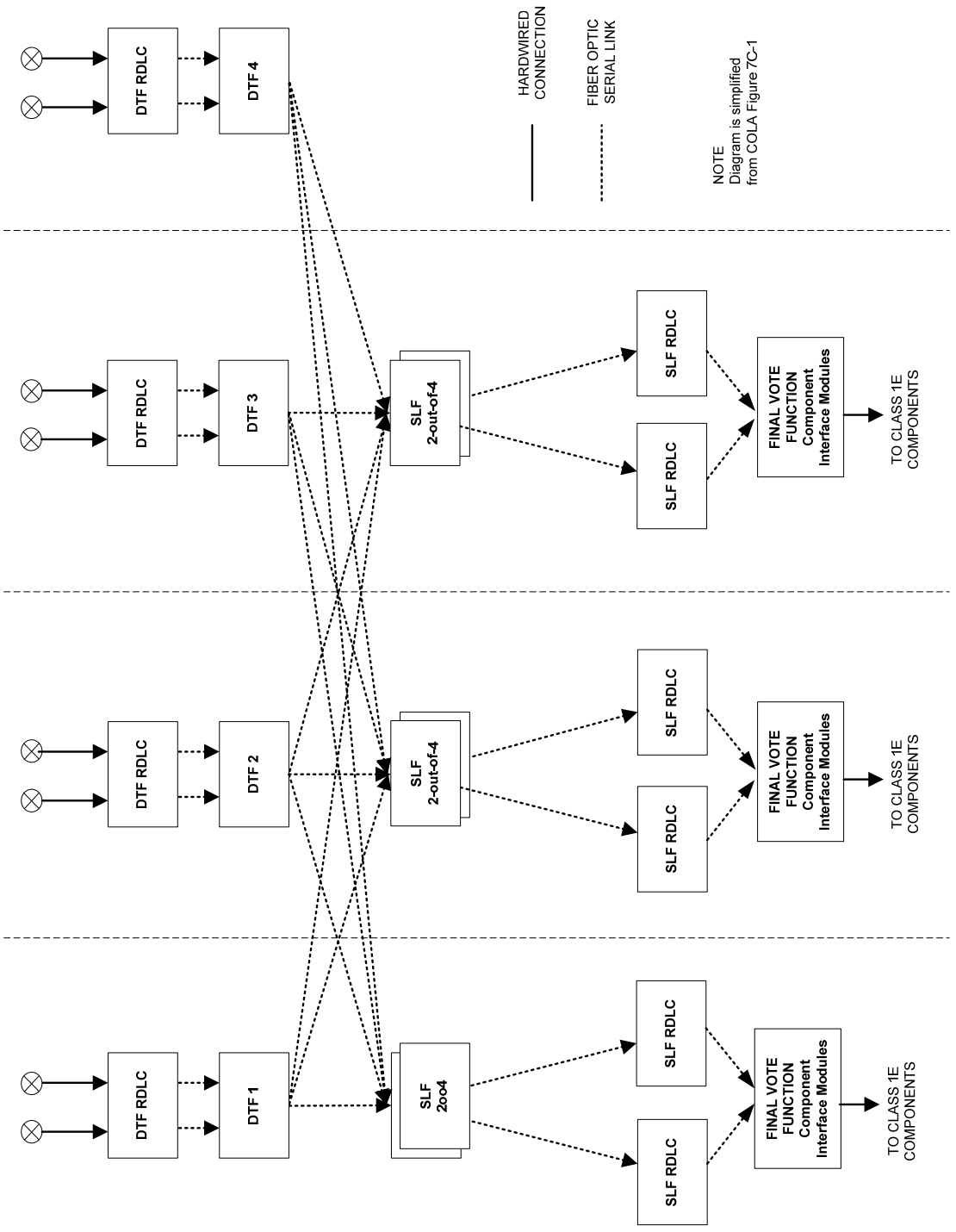


Table 7DS-4 ELCS ESF Inter-division Communication Simplified Block Diagram