7.1S Instrumentation and Control Systems and Platforms

This supplemental section provides information for safety-related and nonsafety-related instrumentation and control (I&C) systems and platforms.

7.1S.1 Field Programmable Gate Array Based Platforms

The Reactor Trip and Isolation System (RTIS) and the safety-related portion of the Neutron Monitoring Systems (NMS) are Non-Rewritable (NRW)-Field Programmable Gate Array (FPGA)-based systems. NRW-FPGA based systems are configurable logic devices that process digital signals in a deterministic way.

7.1S.1.1 Reactor Trip and Isolation System

The Reactor Trip and Isolation System (RTIS) provides the logic and control functions for the Reactor Protection System (RPS) and Main Steam (MS) isolation. RPS is described in greater detail in Section 7.2. The RTIS is one part of the Safety System Logic and Control (SSLC).

The RTIS consists of modules for Digital Trip Functions (DTFs), Trip Logic Functions (TLFs), Output Logic Units (OLUs), and Load Drivers (LDs). The RTIS also contains a separate module for Suppression Pool Temperature Monitor (SPTM). The SPTM is described in Section 7.6.1.7.

The RTIS contains four redundant divisions of DTFs. The DTFs take digitized sensor information from sensors or the SPTM as input. For each system function, the DTF is a comparison of inputs to pre-programmed threshold levels (i.e., setpoints) for possible trip action. The result of the DTF is a discrete trip decision for each setpoint comparison. Each safety division performs the same DTF trip decision based on the independent inputs associated with its own division.

The trip decisions from the DTF in each division are used as input to the TLF performed by each of the four safety divisions. The DTF trip decision results are passed to other divisions through isolated communication links as described in Section 7.9S. The TLF processes DTF trip decisions from all four safety divisions resulting in trip output decisions based on 2-out-of-4 coincidence logic format. The logic format is fail-safe (i.e. loss of signal causes trip conditions) for the TLF and associated DTF. Loss of signal or power to a single division's equipment performing the TLF causes a tripped output state from the TLF, but the 2-out-of-4 configuration of the actuator load drivers prevents simultaneous deenergization of both pilot valve solenoids.

The TLF also receives input directly from the Neutron Monitoring System (NMS) and manual control switches. The details of the NMS system are provided in Section 7.6.1.1.

The trip coincident logic output from the TLF is sent to Output Logic Units (OLUs). The OLUs use devices that provide a diverse interface for the following manual functions:

- Manual reactor trip (per division: 2-out-of-4 for completion).
- MSIV closure (per division: 2-out-of-4 for completion).

- MSIV closure (eight individual control switches).
- RPS and MSIV trip reset.
- TLF output bypass

The OLUs distribute the automatic and manual trip outputs to the MSIV pilot valve and scram pilot valve actuating devices and provide control of trip seal-in, reset, and TLF output bypass (division-out-of-service bypass). Bypass inhibits automatic trip but has no effect on manual trip. The OLUs also provide a manual test input for de-energizing a division's parallel load drivers (part of the 2-out-of-4 output logic arrangement) so that scram or MSIV closure capability can be confirmed without solenoid de-energization. The OLUs are located external to the TLU equipment that implements the TLF so that manual MSIV closure or manual reactor trip (per division) can be performed either when a division's logic is bypassed or when failure of sensors or logic equipment causes trip to be inhibited.

If a 2-out-of-4 trip condition is satisfied within the TLF, all four divisions' trip outputs produce a simultaneous coincident trip signal (e.g., reactor trip) and transmit the signal through hardwired connections to OLUs that control the protective action of the final actuators. The load drivers for the solenoids are themselves arranged in a 2-out-of-4 configuration, so that at least two divisions must produce trip outputs for protective action to occur.

Bypass logic implemented by RTIS is described in Section 7.2.1.1.4.1(2) and shown on Figure 7.2-2.

Each of the four RTIS divisions are powered from their respective divisional Class 1E power supply. In the RTIS, independence is provided between Class 1E divisions, and also between the Class 1E divisions and non-Class 1E equipment.

7.1S.1.2 Neutron Monitoring System

A detailed description of the Neutron Monitoring System (NMS) is provided in Section 7.6.1.1 for safety related functions.

7.1S.1.3 Platform Description

The Reactor Trip and Isolation System (RTIS) and the safety-related portion of the Neutron Monitoring Systems (NMS) are implemented using Non-Rewritable (NRW)-Field Programmable Gate Array (FPGA)-based platforms.

Each FPGA-based system is a modular, chassis-based, rack-mounted system. FPGA-based systems are built as units, which provide the chassis and backplanes. The units perform specific functions, based on the modules placed in the backplane. Therefore, each module has unique architectural features, based on the differences in interfaces and requirements. The module design is implemented using only FPGAs. The design uses relatively simple medium-scale integrated discrete logic chips for all simple logic functions, such as a monostable multivibrator to implement a watchdog timer. Data is transferred between units over optical links.

Each module consists of one or more printed circuit boards and a front panel. The purpose of the front panel is to fix boards to the unit and to provide mounting for a Human-Machine Interface (HMI) and setpoints adjustment. The FPGA-based system also includes power supplies, analog and digital input/output modules, status modules, and all cabling and wiring necessary for operation. Each circuit board can contain one or more FPGAs.

The FPGA-based systems use logic chips that can be configured. The logic is physically embedded in FPGA chips using special tools. The logic is built from simple functional elements (FEs) that are designed to perform simple logic functions that can be combined and arranged in specific patterns to perform signal processing and logic operations, and thus construct the logic necessary to perform a defined function. Once the logic is embedded, the logic is hard coded and cannot be changed. After the logic is defined and embedded, the FPGA components are treated as hardware. An FPGA can only implement digital logic.

The FPGA-based system has self-diagnostic functions that continuously verify proper FPGA and communications performance and provide outputs used to alert the operator.

Each FPGA-based systems have the following attributes:

- Intra-Division Communication

  Data is transferred between units over optical links by the communication modules. The safety-related system has a one-way optical communication data link, providing fixed data sets to each safety-related system and to the nonsafety-related system with Class 1E to non-Class 1E isolation. RTIS offers no possibility of data transfer from the nonsafety to the safety equipment.

- Input / Output (I/O)

  There are I/O modules that are located in the units. Analog Output (AO) modules have analog outputs of up to 16 channels. There are several types of AO modules for different output ranges. AO Module provides electrical isolation capability from safety to nonsafety system. Digital I/O modules have four digital inputs and 16 digital outputs. External inputs and internals are isolated using photo couplers and solid-state relays.

- Power Supply

  The power supply module provides low voltage direct current (DC) power for equipped modules in each unit. The safety-related system has redundant power supply modules in each unit. The RTIS equipment is divisionally powered from multiple Class 1E power sources, one of which is DC backed.

7.1S.2 Microprocessor Based Platforms

The Engineered Safety Features and Control System (ELCS) will be implemented with a microprocessor based platform.

7.1S.2.1 Engineered Safety Features Logic and Control System (ELCS)

The Engineered Safety Features Logic and Control System (ELCS) provides the instrumentation and control functions of automatic actuation, control and display for the Engineered Safety Features (ESF) systems.

The ELCS contains four redundant divisions of Digital Trip Functions (DTFs). The four divisions of DTF safety function actuation status are communicated to three divisions of Safety Logic Functions (SLFs), which correspond to the three divisions of ESF actuated equipment. Each SLF performs two-out-of-four logic on the four redundant DTFs. The DTF to SLF communication and isolation features are described in Section 7.9S.

Each ELCS division is powered from independent power sources.

For the four redundant divisions of ELCS DTFs, any single division of sensors from one DTF can be manually bypassed, causing the ESF safety function actuation logic in the SLFs to become two-out-of-three, while the bypass state is maintained. The bypass status is indicated in the main control room until the bypass status is removed. Only one division can be placed in bypass. An interlock rejects attempts to remove more than one division from service at a time.

As shown in Tier 1 Figure 3.4B, each of the three ESF component actuation divisions contains a minimum of two SLFs. The SLF logic for ECCS functions (i.e. initiation of Reactor Core Isolation Cooling, High Pressure Core Flooder or Automatic Depressurization) is implemented using two redundant SLF processing channels per division. The two redundant channels receive the data from the four redundant divisional DTFs, manual control switch inputs and contact closures. The two redundant SLF processing channels perform the same ESF safety function action logic. One of the two SLFs processes initiation logic for functions that service the reactor vessel at low pressure (e.g. RHR), while a second SLF provides the same support for the vessel at high pressure (e.g. Reactor Core Isolation Cooling (RCIC system and High Pressure Core Flooder (HPCF)) system).

The two redundant SLF processing channels must agree for initiation of the ESF safety function to occur. Two SLF processing channels are used to prevent the inadvertent system level actuation of the ESF safety functions that inject coolant to the core or depressurization.

However, in the event of a failure detected by self diagnostics within either processing channel, a bypass (ESF output channel bypass) is applied automatically (with manual backup) such that the failed SLF processing channel is removed from service. SLF processing channel failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator is able to manually bypass the failed channel.

The two-out-of-two voting of the two SLF processing channels is performed on a component basis with non-microprocessor based equipment or with a separate actuation for a valve from one SLF processing channel and a related pump actuation

from the second SLF processing channel, where both are required to initiate coolant injection.

As shown in Tier 1 Figure 3.4b, each ELCS division includes the following major elements:

- Sensors provide signal input to the ELCS. For ELCS safety functions, the appropriate sensors are connected to the Digital Trip Function.
- The Digital Trip Function receives input signals directly and also receives remote input signals from a Remote Digital Logic Controller (RDLC). The RDLC communicates the remote input signals to the DTF utilizing high speed serial link (HSL) communication with redundant fiber optic modems and optical data cable. HSL communication is described in Section 7.9S.
- The DTF provides a comparison of signal inputs to associated setpoints to determine the trip status for each ESF safety function. The DRF communicates trip status to the Safety Logic Functions (SLFs) in each division by means of optical-based HSL communication links.
- Individual DTF to SLF communication is provided with single fiber optic cable since the DTF and SLF are both located in the MCR area.

SLFs are provided in each of the three ESF divisions that provide electromechanical component actuation. Each division's SLFs receive ESF safety function actuation status signals from each of the DTFs in the four redundant divisions. The division's SLFs calculate ESF system level actuation status by determining whether there is a two-out-of-four coincidence of DTF ESF safety function trip signals. The SLF also receives hardwired signals for manual bypass and manual system level actuation of ESF components from I/O that is local to the SLF. The SLF communicates ESF actuation commands to the SLF I/O stations that are located in areas that are remote from the MCR by HSL. The fiber optic cables are redundant for the communication of ESF safety function actuation commands from the SLF to the SLF remote I/O.

The SLF Remote Digital Logic Controller (RDLC) provides I/O and ESF component control logic and actuation. At the RDLC a Component Interface Module (CIM) is provided for each controlled electromechanical component assigned to the SLF. The CIM interfaces the ESF actuation command signals (or control commands in the absence of actuation) from the SLFs to the electromechanical ESF component.

The CIM provides priority logic to override control when an ESF actuation occurs. Logic in the CIM also provides voting of redundant SLF processing channels signals, for ESF safety functions that require SLF redundancy. The CIM receives component position and status feedback signals from the component control circuit. The CIM provides local control capability for maintenance.

Each ELCS division has an intra-division network that connects the ELCS controllers with flat panel safety displays in the main control room and a Maintenance and Test Panel. The intra-division network is described in section 7.9S.

For each ELCS division, there are two safety display stations in the main control room. Each safety display is driven by a flat panel display subsystems.

Each ELCS division has a permanently connected Maintenance and Test Panel (MTP) and an Interface and Test Processor (ITP). The MTP and ITP are utilized for the maintenance technician functions.

7.1S.2.2 ELCS Platform

The platform that implements the ELCS has the following major elements:

- Controller, including high speed serial link communications
- Intra-division Network communication
- Input / Output
- Flat Panel Display
- Maintenance and Test Panel
- Power Supplies
- Component Interface Module

The ELCS Controller subsystem is modular. A passive backplane connects individual module slots, which can house the following module types:

- Controller module
- Intra-division communication module
- Input / Output modules

7.1S.2.3 ELCS Controller

The controller contains two sections, a processing section and a communication section. The processing section contains a microprocessor and memory for the applications programs. The processing section memory utilizes Flash PROM for system software, Flash PROM for application software, and RAM.

The communication section contains another microprocessor and memory for communications with other Controllers in different chasses. The communications memory utilizes Flash PROM for system software and RAM. The communications section performs the HSL communications functions and the HSL diagnostics.

The two controller sections communicate through shared memory. The shared memory provides for communications isolation. The ELCS Controller performs self-diagnostics, including an internal watchdog timer, and is able to determine that the required module types are located in the appropriate slot.

The backplane allows multiple Controllers to be utilized in a single chassis. The controllers communicate through shared memory that is located on the Intra-division communication module.

- Intra-Division Communication

  The communication module provides the interface for the intra-division communication network. The intra-division performs communication diagnostics, Intra-division communications are described in Section 7.9S.

- Input / Output

  The Controller uses compatible I/O modules that are located in the chassis with the controller. Additional chasses of I/O modules can be added to the first Controller chassis if additional I/O is necessary. A range of modules is available covering analog and digital signals of various types. In addition, there are modules for temperature measurement and rotational speed measurement.

  The system software in the Controller automatically checks that all modules are operating correctly at system startup. Module diagnostic failures are reported to the Controller.

- Flat Panel Display

  The flat panel display subsystem consists of the flat panel display with touch screen capability, a single board computer, and standard communication interfaces for communication to the intra-division network.

  For STP Units 3 and 4, the RTIS and NMS utilize the ELCS flat panel display subsystem to display selected information. Each division of RTIS and NMS send data to a communication interface associated with the same ELCS division. The RTIS and NMS utilized serial fiber optic data links over fiber optic media. The communication interface then communicates the RTIS and NMS information to an interface module on each flat panel display subsystem. The data flow is unidirectional from RTIS and NMS to the ELCS communication interface.

- Maintenance and Test Panel (MTP)

  The MTP will be used for technician surveillance, maintenance and test functions for each division. The MTP provides the means for the operator or technician to change setpoints, insert and remove bypasses, support periodic testing, and display detailed system diagnostic messages. The MTP provides features that support the administrative control for the activities.

  The MTP utilizes a flat panel display subsystem in conjunction with the ITP for monitoring diagnostics and providing a periodic test interface for other Controllers. The MTP and ITP are connected to the intra-division network.

  The MTP flat panel display subsystem also includes a communication interface to the nonsafety system. The MTP communication interface to the nonsafety systems provide for communication isolation to assure that data flows in a unidirectional manner from the ELCS to the nonsafety systems. The communication interface

utilizes an optical connection to the nonsafety systems to provide electrical isolation.

- Power Supply

  The power supply subsystem provides low voltage direct current (DC) power for the ELCS equipment that requires it. ELCS equipment is divisionally powered from multiple Class 1E power sources, one of which is DC backed.

- Component Interface Module (CIM)

  In general, the CIM provides the interface between the ELCS actuation and control command signals and the electromechanical device associated with the final ESF components. Electromechanical components with non-standard signal interface requirements may not use a CIM, but could be interfaced with discrete I/O.

7.1S.3 Plant Information and Control System (Non-Safety)

The Plant Information and Control System (PICS) provides integrated process control, monitoring, and human-system interface functions for the nonsafety-related plant process systems. PICS includes computer workstations for the human interface and data processing, controllers and servers for the process control functions, and a real-time communications network to share data between the different controller and computer processors. Typical data communication interfaces to PICS are illustrated in Figure 7.9S-1.

The Plant Computer Functions (PCFs) are a set of functions that were provided by the Process Computer System (PCS) in the original ABWR DCD design. The STP 3&4 design does not have a PCS. These PCFs are a subset of PICS and include data display and alarms, plant computer calculations (e.g., Power Generation Control System (PGCS)) and data recording (logging) (see Subsections 7.7.1.5, 7.7.2.5 and 7.7.1.2.2 (6)), and historical archiving (including Sequence of Events). The PCFs have not changed from those of the ABWR DCD Process Computer System.

The PICS is configured as a distributed control system (DCS). Therefore, PICS, as a DCS, is an integrated set of control processors, servers, workstations, and applications that provide plant wide process control and monitoring. PICS also acts as the supervisory control system and provides the primary interface between the control room operators and the plant process and equipment data and control capabilities. Several computer processors are linked together via a real-time communications network, sharing the computer processing tasks.

Each computer processor transmits and receives data from the communications network. Each device in the network receives the same data at essentially the same time, creating a network database that is shared by each of the computer processors.

PICS has the following major elements:

- Control processors and servers

- Workstations
- Network Communications
- Input/Output Modules
- Video Display Units