7.9 Data Communication Systems

7.9.1 Description

This section addresses both the essential (safety-related) and non-essential (nonsafety-related) data communication functions, as specified in RG 1.206, that are part of or support the instrumentation and control (I&C) systems described in Sections 7.1 through 7.8. This includes data communication between systems and between divisions within a system. Communication within a system is an integral part of that system.

The Data Communication Functions (DCFs) of the Reactor Trip and Isolation System (RTIS), Neutron Monitoring System (NMS), and ESF Logic and Control System (ELCS) are required to support the safety-related functions of these systems. The DCFs of these systems are an integral part of these systems.

The majority of the non-essential data communications are performed through a plant-wide distributed data network defined as the Plant Data Network (PDN). The PDN provides the distribution of process and other data required to support the nonsafety-related operational functions.

Figure 7.9-1 provides an overview of the ABWR data communication configuration.

7.9.2 Data Communication Functions (DCFs) of the SSLC Systems

7.9.2.1 Safety-Related Functions

The safety-related DCFs (also termed Essential Communication Functions (ECFs)) associated with the Safety System Logic and Control (SSLC) systems perform data collection and data distribution using both local and remote data acquisition and control units connected by dedicated data links and/or networks for each of the following systems, segments, and divisions:

- RTIS (4 divisions)
- NMS (4 divisions)
- ELCS (4 divisions), including the safety-related Main Control Room panel displays
- Other safety-related I&C platforms (divisions as described in other FSAR sections)

7.9.2.2 Nonsafety-Related Functions

The safety-related digital systems described here also provide the following nonsafety-related communication functions:

- Provide alarm and status data from safety-related plant sensors and the SSLC systems to the nonsafety-related Plant Information and Control System (PICS) for Main Control Room (MCR) indication and computer logging through isolated interfaces and the PDN.

- Provide selected safety-related plant process data to the nonsafety-related control systems through isolated interfaces. The interconnection of Class 1E communication to non-Class 1E devices is done using fiber optic cable. The fiber optic cable provides the necessary electrical isolation. Communication to nonsafety-related systems are controlled by the safety device to assure no communication task will interfere with the safety system performing intended functions.

- Provide for the transfer of the NMS calibration data from the nonsafety-related PCF to the NMS. Plant personnel action to manually accept the data transfer to the operational safety side is required for such data to be accepted.

7.9.2.3 Communication Within a Division

The safety-related data communication is based on serial, point-to-point data transmission. The transmission is purely unidirectional without acknowledgment from the other side. The transmitting and receiving devices are optically isolated from each other. The integrity of the links and the data transmitted is monitored by the receiver. The data transmission cycle time is fixed and the communication is deterministic. Self diagnostics are used to monitor the proper operation of data links.

Use of a system or segment data communication function to communicate command and control signals to final actuators varies by each system or segment. ELCS provides control signals to remote input/output devices through its data communication links. RTIS inputs and control outputs are directly connected to field devices. NMS provides no control signals to final actuators, but does provide direct connected trip data to RTIS.

Safety-related data communication is used by RTIS and NMS to transmit safety related display information to the ELCS.

The ELCS utilizes a deterministic network within each division to support main control room safety related displays and maintenance and test functions.

7.9.2.4 Communication Between Divisions

For RTIS and ELCS, limited communication between divisions is necessary. For example, individual divisional input trip determinations must be shared between divisions in order to support two-out-of-four voting for divisional trip outputs. To support this, there are a limited set of dedicated data communication links from each division to each of the other divisions. The links provide a qualified and isolated, point-to-point, single direction communication path between divisions so as to preserve divisional independence.

The NMS does not rely on data communication between divisions.

7.9.2.5 Design-Basis Information

The safety-related DCFs (also termed ECFs) have the following safety design basis:

- Provide for the transmittal of data between input/output (I/O) devices, (locally and remotely) and controllers. This allows process information, equipment status information, and operator input to be made available to controllers for the processing of safety-related control functions, and making the controller output information available to I/O devices for distribution to final actuators and operator interfaces.
- Provide for the transmittal of data between divisions or from safety-related systems to nonsafety-related systems through qualified isolation devices such as fiber optic communication.
- Provide data communication that is predictable and verifiable (deterministic) and that does not compromise the functionality of either the transmitting or receiving system.

7.9.2.5.1 Quality of Components and Modules

Applicable quality assurance provisions of 10 CFR 50 Appendix B, IEEE-603 and IEEE-7-4.3.2 are applied to the SSLC systems, of which the ECFs are integral parts.

7.9.2.5.2 Software Quality

Development of software for the safety system functions within the SSLC systems, including their ECFs, conforms to the guidance of IEEE-7-4.3.2 and Branch Technical Position BTP-HICB-14 as discussed in Appendix 7B to this chapter.

7.9.2.5.3 Protocol Support of Performance Requirements

The real-time performance of SSLC systems, including their ECFs, in meeting the requirements for safety system trip and initiation response conforms to BTP-HICB-21. Each communication interface operates independently and asynchronously with respect to other communication interfaces. Maximum time delay from input to output is deterministic, based on the control logic and communication design. Data rates (bandwidth) are constant as the communication modules provide the same data elements to each destination at the prescribed frequency. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division. Timing requirements of IEEE-603 are also met.

7.9.2.5.4 Reliability

The simplicity of the communication design, combined with self diagnostics make the ECFs of the SSLC highly reliable. The two-out-of-four logic prevents any single error from causing or preventing an actuation of functions.

Errors are detected by self-diagnostic tests (i.e. checksum, parity check, or reception of a keep-alive signal). Should data not be available, the logic takes predetermined action based on the specific data involved.

7.9.2.5.5 External Access Control

There are no unprotected electronic paths by which unauthorized personnel can change plant software or display erroneous status information to the operators. Interfaces external to the plant are through security protected interfaces that allow communication between the nonsafety PDN to the offsite Emergency Operations Facility (EOF). Although the EOF Workstation contains login protection (passwords or other protective measures), the data access control resides in the site security protected interfaces and data servers.

The SSLC ECFs are additionally protected by isolated interfaces to the nonsafety PDN that only allow one-way data transfer from the safety to nonsafety network. The SSLC networks have no direct external electronic paths.

7.9.2.5.6 Single Failure Criterion

The ECFs of the SSLC systems satisfy the requirements of the single-failure criterion through conformance to IEEE-603, IEEE-379 and Regulatory Guide 1.53. Communication between divisions preserves divisional independence such that a failure in one division does not affect other divisions.

7.9.2.5.7 Independence

The ECFs of the SSLC systems satisfy the requirements for independence through conformance to Clauses 4.6 and 4.7 of IEEE-279, IEEE-384, IEEE-603, and Regulatory Guide 1.75. Divisions are physically separated and electrically isolated from each other. Divisions have separate power sources. Transmission of logic signals between divisions is through qualified isolation devices.

NMS can receive calibration data from nonsafety-related maintenance support systems. On a divisional level, a division must be manually placed in inop and manually verified and accepted before such data is allowed in the portion of the device performing the safety function. Only limited data in a strict format will be accepted by the safety device.

To meet the requirements of IEEE-384 and Regulatory Guide 1.75, the protective covering of the fiber optic-based cables are flame retardant. The cables are passed through physical, safety class barriers, where necessary, for separation of Class 1E circuits and equipment from other Class 1E equipment or from non-Class 1E equipment. The ECF equipment is kept physically separate to minimize the effects of design basis events. During operations, the functionality of the ECFs of SSLC, NMS and RTIS is independent of nonsafety systems.

7.9.2.5.8 Protection System Failure Modes

The RTIS and NMS systems are designed to fail into a safe state upon loss of communications. ELCS fails as-is during communication failure, that is, system controllers continue to operate based on the last command.

7.9.2.5.9 Testing and Surveillance

The safety-related DCFs (ECFs) are integral functions of the SSLC systems. SSLC testing features and surveillances encompass those related to the ECFs. SSLC testing and surveillance is covered in 7.1.2.1.6.

7.9.2.5.10 Bypass and Inoperable Status Indications

The safety-related DCFs (ECFs) are integral functions of the SSLC systems. SSLC bypass and inoperable status indications encompass those related to the ECFs that provide information for compliance with RG 1.47.

7.9.2.5.11 Isolation Protection

Fiber optic-based isolation devices are expected to have less difficulty than previous isolation devices in complying with all qualification requirements due to their small size, low mass, and simple electronic interfaces. The basic materials and components, except for the fiber optic cable itself, are the same as those used in existing, qualified isolation devices. A major advantage of fiber optics is that signals can be transmitted long distances and around curves through the isolating medium; thus, the physical, safety-class barrier required for separation of Class 1E devices may be provided by just the cable length if the protective covering and any fill materials of the cable are made properly flame-retardant. For short distances, the fiber optic cable can be fed through a standard safety class structure.

7.9.2.5.12 Diversity and Defense-in-Depth

Diversity and defense-in-depth is covered in Appendix 7C. FMEA is discussed in Appendix 15B.

7.9.2.5.13 Seismic Hazards

All of the equipment implementing the ECFs of the SSLC is located in Seismic Category I structures and meets RG 1.100 and IEEE 344.

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

7.9.2.6 Analysis

7.9.2.6.1 General Requirements Conformance

The ELCS, RTIS and NMS each have safety-related data communication functions for data collection and data distribution. Each system provides four independent communication functions to serve the four divisions of plant protection and safety systems and safety- related display systems. These communication functions are classified as safety-related since they are considered integral parts of the safety-related systems that they serve.

7.9.2.6.2 Specific Regulatory Requirements Conformance

The safety-related DCFs are integral functions of the SSLC systems. Conformance to specific regulatory requirements related to the safety-related DCFs is addressed in the sections related to the SSLC systems.

7.9.3 Plant Data Network (PDN)

7.9.3.1 Plant Data Network (PDN) Functions

The Non-Essential Communication Functions (NECFs) support the data communications for non-safety-related plant functions. The NECFs are implemented through the use of a distributed Plant Data Network (PDN). The PDN provides a plant wide, highly reliable, high speed data communication network for plant control, monitoring, and other related operational needs.

The PDN is nonsafety-related and supports the collection and distribution of data for multiple systems using a layered network design. A control layer is designated for systems and information that directly impact plant operation. The PDN has other communication layers that support other selected nonsafety-related functions.

The control network supports data communication between:

- Process I/O units, controllers, engineering workstations
- Network monitoring, historical data storage units, control building workstations
- Main control room panel displays and workstations that support the operator interfaces
- Printers
- Network gateways that support the one-way acquisition of data from the safety systems for plant data historian recording and for use on nonsafety displays.

The PDN supports data communication to workstations for the Technical Support Center (TSC), the Emergency Operations Facility (EOF) and other external data users (e.g., engineering offices). External connectivity is limited and only provided from the network through a security protected interface.

The PDN is designed around a fully redundant, fiber-optic based backbone. The backbone is defined as the cabling between the core switches and between the core and zone switches. The PDN provides sufficient throughput capacity to support all of the data communication needs including the PICS needs to acquire, process and store data at the required scan and processing rates from available data sources, as well as support displays.

7.9.3.1.1 PDN System Interfaces

The PDN interfaces with the controllers, gateways, communication interface modules, engineering workstations, main control panel workstations and printers through zone switches. The PDN also interfaces with the ELCS and RTIS through isolated interfaces that only allow one-way data transfer from the ELCS and RTIS to the PDN. The isolation method is through the use of fiber optic-based communication that does not have the capability of receiving communications from the transmitting source. Interface to the NMS is explained in 7.9.2.2.

The PDN also interfaces with the TSC and EOF through a security protected interface, for example a firewall.

7.9.3.1.2 PDN Classification

The PDN is classified as nonsafety-related. The PDN is essential to power generation through its data communication support of operation and the power generation systems control and monitoring functions performed by other equipment.

7.9.3.1.3 PDN Power Sources

Two separate Non-Class 1E feeds from the Non-Class 1E 120 Vital AC (VAC) or 125 VDC systems power the PDN. This redundancy allows the PDN to operate such that any single failure in the system power supplies will not cause the loss of data communications to the interfacing systems or equipment.

The power sources automatically switch over upon failure of one power source or power supply module.

7.9.3.1.4 PDN Equipment

PDN hardware includes core switches, zone switches, security devices, mounting cabinets, patch panels, fiber-optic cables and associated junction boxes and cable supports.

7.9.3.1.5 PDN Testability

Network monitoring is an integral part of the PDN and provides the capability to continuously monitor network operation and performance. Network monitoring workstations allows system management, test, and control of the PDN functions.

7.9.3.1.6 PDN Environmental Considerations

The PDN is designed to operate in the normal plant environment where it is located. Its support function serves power generation purposes only. It is not required for safety purposes and is not required to operate after a design basis accident.

7.9.3.1.7 PDN Operational Considerations

No operator actions are required since the system is capable of self-starting following power interruptions, or any other single failure, including any single switch failure. After repairs or replacements are performed, PDN equipment automatically re-initializes to normal status when power is restored.

7.9.3.1.8 PDN Operator Information

The self-test provisions of the PDN are desired to alert the operator to system anomalies via alarms. Problems are alarmed . The system is designed such that no control output or alarm is inadvertently activated during system initialization or shutdown.

7.9.3.2 PDN Design Basis Information

The PDN has no safety design basis.

General Design Functions

The PDN provides a plant wide distributed data communication networks to support the plant control and monitoring (nonsafety-related) systems. The PDN includes the active electrical components and connectivity (such as switches and cabling), between the components defined by other plant systems. The PDN also includes the associated communication software required to support its function of providing plant-wide data for distributed control and monitoring.

The PDN is the means by which process data is distributed to the various nonsafety-related plant control and information systems requiring data and to the main control room for processing and display.

(1) System Interface

The PDN control network interfaces with nonsafety-related controllers, gateways, communication interface modules, engineering workstations, main control panel workstations, and printers through zone switches.

(2) Classification

The PDN, of itself, is neither a power generation system nor a protection system. It is a data communication network utilized for transmission of data for power generation (nonsafety-related) systems. It is classified as nonsafety-related.

(3) Power Sources

The PDN receives its power from two separate non-Class 1E distribution panels from the non-Class 1E 120 VAC UPS and 125 VDC. This redundancy allows the PDN to supply dual logic functions such that any single failure in the system power supplies will not cause the loss of the validated outputs to the interfacing actuators and to the monitors and displays.

(4) Equipment

The PDN hardware is comprised of fiber optic-based or direct connection cabling, switches, security devices and gateway devices. These interface with the PICS control devices and gateways.

(5) Diagnostics and Testability

The PDN contains built in, continuously running, self-diagnostic capabilities to sense and correct or block data and device errors. Faults or problems are logged and alarmed.

(6) Environmental Considerations

The PDN is not required for safety purposes, nor is it required to operate after the design basis accident. Its support function serves power generation purposes only and it is designed to operate in the normal plant environment.

(7) Operational Considerations

The PDN automatically initiates for both cold and warm starts. No operator actions are required in that the PDN is capable of self-starting following power interruptions, or any other single failure, including any single processor failure. After repairs or replacements are performed, the PDN automatically re-initializes to normal status when power is restored to any unit and automatically resets any alarms.

(8) Operator Information

The self-test provisions are designed to alert the operator to system anomalies via interfaces with the PICS. The circuitry is designed such that no communication is inadvertently activated during network initialization or shutdown. For such events, control outputs change to predetermined fail-safe outputs.

The PDN has the following nonsafety-related design bases:

- Transmits data between controllers.

- Allows for process and equipment status information and operator input to be available to controllers for the processing of nonsafety-related control functions.
- Provides for the receipt of data from the safety-related DCFs through isolated interfaces to nonsafety-related workstations, controllers and historians for the purposes of display and alarm to operators, transient analysis and sequence-of-events recording and nonsafety-related control functions.
- Provides for the transmission of data to interfaces with the Technical Support Center (TSC) and Emergency Operations Facility (EOF).

7.9.3.3 Analysis

7.9.3.3.1 General Requirements Conformance

The PDN constitutes neither a power generation system nor a protection system, by itself. It is a support function utilized for the transmission of data for power generation (nonsafety-related) systems and their associated sensors, actuators and interconnections. The PDN equipment is classified as nonsafety-related and does not interface with any engineered safeguard or safety-related system except for the reception of isolated signals for alarm, display or nonsafety-related control purposes as discussed in Subsection 7.9.2.2. The PDN supports power generation systems. As such, it meets the same functional requirements imposed on those systems. Although not required to meet the single-failure criterion, the PDN equipment is redundant and receives its power from redundant, highly reliable power sources such that no single failure will cause its basic function to fail.

The PDN equipment and software is also diverse from those implementing the safety-related DCFs of the SSLC systems (different hardware and/or software) to minimize the effect of common-mode failures as discussed in IEEE 7-4.3.2.

7.9.3.4 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with Section 7.9 of the Standard Review Plan. It provides specific enhancement for control systems in their conformance with GDCs 13 and 19.

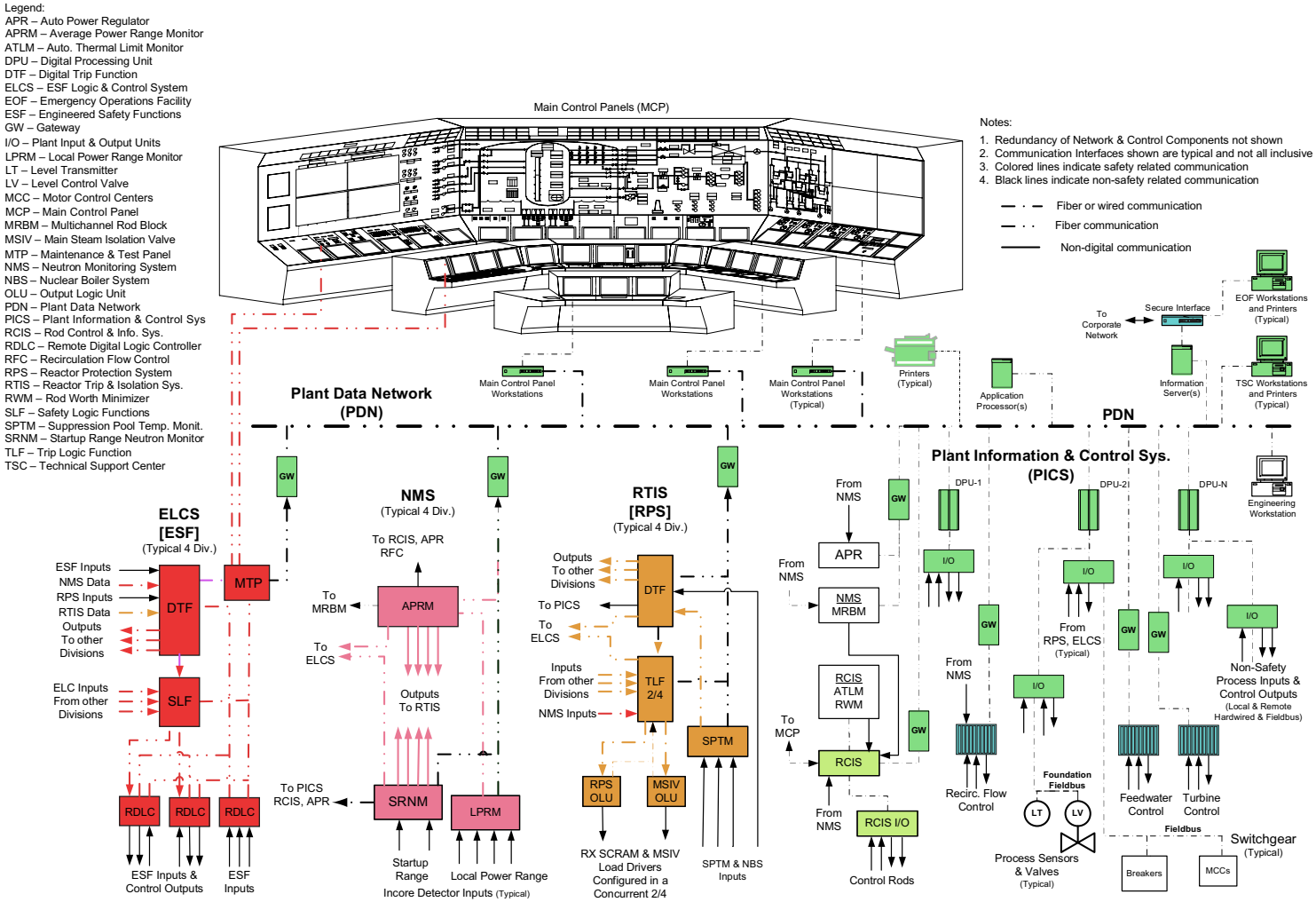

Figure 7.9-1 Data Communication Interface