7.9S Data Communication Systems

7.9S.1 Description

This section addresses both safety and non-safety related data communication functions that are part of or support the instrumentation and control (I&C) systems described in Sections 7.2 through 7.8. This includes data communication between systems, internal to a system and between divisions within a 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-safety related data communications is performed through a plant wide distributed data network defined as the Plant Data Network (PDN). The PDN supports the plant-wide distribution of process and support data required to support the non-safety related operational functions, including the non-safety related functions of displaying and recording data. The PDN is a stand-alone system and is covered in Sections 7.7.1.9 and 7.7.2.9.

7.9S.1.1 Data Communication Functions (DCFs) of the SSLC Systems

The DCFs associated with the Safety System Logic and Control (SSLC) systems perform data collection and data distribution using independent distributed data acquisition and control networks for each of the following systems, segments and divisions:

(1) RTIS (4 divisions)

(2) NMS (4 divisions)

(3) ELCS, including the safety-related Main Control Room Panel displays (4 divisions)

These DCFs are not systems, but are integral functions of the system segment that they serve. The RTIS, NMS and ELCS systems provide all of the electrical devices and circuitry, such as data communication physical connections and controllers, to establish communications between sensors, display devices, controllers and actuators, as defined by plant safety system design.

The safety-related data communications are based on high speed networks that use a reflective memory type design, employing redundant, counter-rotating, fiberoptic rings. Each processing node on a network has associated with it, reflective memory that holds current data values for all signals from all processors present on that same network. Processors write their current data values to their own reflective memory. All data from each processor's reflective memory is written to all other reflective memory on the same network on a fixed determinisitic frequency. This assures that sensor data and control data are guaranteed network access without interference from other network traffic. Data communication between reflective memory is done over dual, counter-rotating fiberoptic rings, assuring that all data continues to be written to all reflective memory modules on the network even in the event that both communication

paths break at the same location. These features assure that the data communication is highly reliable (fault tolerant) and deterministic.

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 data communication links from each division to each of the other three divisions. The links provide a qualified and isolated, single direction communication path so as to preserve divisional independence.

Input and output signals between field devices as well as data from intermediate system functions are made available to all other processors on the network. The networks provide both local and remote communication capabilities. In some cases, such as Turbine Building sensor inputs to the RTIS, the sensor signals are hardwired directly to input modules located in the same chassis as the system logic processors, thereby bypassing the communication network. In other cases, such as the Startup Range Neutron Monitor (SRNM) and Power Range Neutron Monitor (PRNM) in the NMS, the data acquisition and primary signal processing is performed in the NMS prior to providing it to other processors on the network.

Use of a system's or segment's data communication network 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 network. RTIS control outputs are directly hardwired to field devices, thereby bypassing its data communication network. NMS provides no control signals to final actuators, but does provide trip data to RTIS over direct point-to-point communicaiton interfaces.

The safety-related communication networks described here also provide the following non-safety related communication functions:

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

(2) Provide selected sensed safety-related plant data to the non-safety-related control systems through an isolated gateway interface.

7.9S.1.2 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. Section 7.7.1.9 provides a description of the PDN.

7.9S.2 Design-Basis Information

7.9S.2.1 Safety-Related DCFs

The safety-related DCFs have the following safety design basis:

> The safety-related DCFs transmit data between input/output (I/O) devices and controllers, making process and equipment status information and operator input available to controllers for the processing of safety-related control functions, and making controller output information available to I/O devices for distribution to final actuators and operator interfaces.

7.9S.2.1.1 Quality of Components and Modules

Applicable quality assurance provisions of 10CFR50 Appendix B and IEEE Std 7-4.3.2 will be applied to the SSLC systems, of which the DCFs are integral parts.

7.9S.2.1.2 Software Quality

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

7.9S.2.1.3 Protocol Support of Performance Requirements

The real-time performance of SSLC systems, including their DCFs, in meeting the requirements for safety system trip and initiation response conforms to BTP-HICB-21. Each controller operates independently and asynchronously with respect to other controllers. Maximum time delay from input to output is deterministic, based on the control logic and communication network design. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division.

7.9S.2.1.4 Reliability

The fault tolerant network architecture and extensive self testing by the processors of the SSLC system make the DCFs of the SSLC highly reliable.

The dual counter-rotating fiber optic ring structure allows communication to continue in the event of any single failure.

7.9S.2.1.5 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. The only interfaces external to the plant are through firewalls that allow only one way transmission from the non-safety PDN to the offsite Emergency Operations Facility (EOF). The SSLC DCFs are additionally protected by gateways to the non-safety PDN that only allow one-way data transfer from the safety to non-safety network. The SSLC networks have no direct external electronic paths.

The digital safety system security guidance provided in Section 2 of Regulatory Guide 1.152, Revision 2 will be adapted to the SSLC DCFs.

7.9S.2.1.6 Single Failure Criterion

The DCFs of the SSLC systems satisfy the requirements of the single-failure criterion through conformance to IEEE-279, IEEE-379 and Regulatory Guide 1.53. There are four independent safety divisions in each of the three independent safety-related communication networks for ESF, RPS and NMS.

7.9S.2.1.7 Independence

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

7.9S.2.1.8 Protection System Failure Modes

The RTIS systems are designed to fail into a safe state upon loss of communications.

7.9S.2.1.9 Testing and Surveillance

The safety-related DCFs are integral functions of the SSLC systems. SSLC self-testing features and surveillances encompass those related to the DCFs.

7.9S.2.1.10 Bypass and Inoperable Status Indications

The safety-related DCFs are integral functions of the SSLC systems. SSLC bypass and inoperable status indications encompass those related to the DCFs.

7.9S.2.1.11 Susceptibility to Electromagnetic and Radio Frequency Interference

The DCFs of the SSLC systems use fiber-optic media, which does not present a fault propagation path for environmental effects, such as high-energy electrical faults and lightning, from one redundant portion of a system to another, or from another system to a safety system. The fiber-optic media is not located in high radiation areas that could degrade its performance.

7.9S.2.1.12 Diversity and Defense-in-Depth

Diversity and defense-in-depth is covered in Appendix 7C.

7.9S.2.1.13 Seismic Hazards

All of the equipment implementing the DCFs of the SSLC is located in seismic Category I structures.

7.9S.2.2 PDN Design Basis Information

The PDN has no safety design basis.

The PDN has the following non-safety related design bases:

(1) The PDN transmits data between input/output (I/O) devices and controllers, making process and equipment status information and operator input available to controllers for the processing of non-safety-related control functions, and making controller output information available to I/O devices for distribution to final actuators and operator interfaces.

(2) The PDN transmits data from the safety-related DCFs through isolated gateway interfaces to non-safety-related workstations, controllers and historians for the purposes of display and alarm to operators, transient analysis and sequence-of-events recording and non-safety-related control functions.

(3) The PDN transmits data to interfaces with the Technical Support Center (TSC) and Emergency Operations Facility (EOF).

7.9S.3 Analysis

7.9S.3.1 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 data acquisition and control networks to serve the four divisions of plant protection and safety systems and safety-related display systems. These communication networks are classified as safety-related since they are considered integral parts of the safety-related systems that they serve.

The general requirements conformance analysis for the PDN is included in Section 7.7.2.9.1.

7.9S.3.2 Specific Regulatory Requirements Conformance

7.9S.3.2.1 Safety-Related DCFs

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

7.9S.3.2.2 PDN

The specific regulatory requirements conformance analysis for the PDN is included in Section 7.7.2.9.2.