ANP-10309 —U.S. EPR Protection System Technical Report

7.3 *Identification of Invalid Signals*

[

]

[

]

- [

  ]

- [

  ]

RAI 505, Question 07.01-36 #6

ANP-10315 —U.S. EPR Surveillance Testing and TELEPERM XS Self-MonitoringTechnical Report Markups

AREVA

Proprietary

ANP-10315NP
Revision 2~~1~~

U.S. EPR ~~Protection System~~ Surveillance Testing and TELEPERM XS Self-Monitoring

RAI 505
Question 07.01-44

Technical Report

______2012

AREVA NP Inc.

Proprietary

This is changed throughout the document in response to Question 07.01-44

1.0 INTRODUCTION

1.1 *Purpose*

This technical report presents the overall surveillance testing philosophy applied to the U.S. EPR ~~Protection System (PS)~~safety-related I&C systems and the diverse actuation system (DAS). The philosophy described herein is consistent with surveillance requirements found in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specifications 3.3.1 and 3.3.4. The overall surveillance testing philosophy is described with particular emphasis on:

- Describing complete testing coverage of the ~~PS~~ safety-related I&C systems via overlapping tests, including self-~~testing~~ monitoring and periodic surveillance testing.
- Providing detail regarding the self-~~testing~~ monitoring features to demonstrate their adequacy.
- Describing compliance with regulatory requirements and conformance to guidance applicable to surveillance testing of the U.S EPR ~~PS~~safety-related I&C systems.
- Describing complete testing coverage of the DAS via overlapping tests.

1.2 *Scope*

The body of this technical report addresses the surveillance testing and self-monitoring of the U.S. EPR ~~PS~~ safety-related I&C systems which, together, provide complete testing coverage from sensor through actuator. The scope of the body of this report corresponds with the technical specification surveillance requirements applicable to the ~~PS, which are~~safety-related I&C systems found in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1. Other I&C systems not discussed in the technical specification surveillance requirements (PAS, RCSL, HMS, etc.) are not addressed as part of this report.

07.01-44

The exception is the hydrogen monitoring system (HMS). This system does not have any technical specification surveillance requirements, but its periodic testing is described in Section 2.2.1 and 2.2.2.

The scope of Appendix A of this report corresponds with the Technical Specification Surveillance Requirements applicable to the DAS, which are found in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.4.

The scope of Appendix C of this report discusses the test of the PACS upon a loss of power condition.

Section 2.2.6 of this report is applicable to any system implemented with Teleperm XS (TXS) micro-processor based technology (e.g., U.S. EPR Safety Automation System (SAS)). ~~The remainder of the report is specific to the U.S. EPR PS.~~ Self-Monitoring features are only credited in the PS and SAS for technical specification surveillance requirements. Other systems may have self-monitoring features, but they are not credited for any surveillance requirements.

The following I&C systems are within the scope of this report:

- Protection System (PS).
- Boron Concentration Measurement System (BCMS).
- Excore Instrumentation System (EIS).
- Incore Instrumentation System (ICIS).
- Priority and Actuator Control System (PACS).
- Radiation Monitoring System (RMS).
- Rod Position Measurement System (RPMS).
- Safety Automation System (SAS).
- Signal Conditioning and Distribution System (SCDS).

07.01-44

- Hydrogen Monitoring System (HMS).
- Diverse Actuation System (DAS).

07.01-44

2.0 U.S. EPR ~~PROTECTION~~ SAFETY-RELATED I&C SYSTEMS SURVEILLANCE TESTING PHILOSOPHY

2.1 *Overview*

Descriptions in this report correspond with the U.S. EPR ~~PS~~ safety-related I&C systems design as defined in ~~ANP-10309P, "U.S. EPR Digital Protection System Technical Report" (Reference 11)~~U.S. EPR FSAR Tier 2, Section 7.1.

The U.S. EPR ~~PS~~ safety-related I&C systems surveillance testing philosophy consists of both periodic testing and self-~~tests~~ monitoring that, together, provide complete coverage from sensor to actuator for reactor trip (RT) and engineered ~~safeguard~~ safety features ~~actuation~~ (ESF) functions. This philosophy takes advantage of comprehensive and wide-ranging self-~~test~~ monitoring features of the TXS platform that render additional periodic testing of some portions of the system unnecessary. Specifically, self-test features replace the traditional channel check and channel functional test surveillances. 07.01-44

- Channel check is performed by an automatic parameter comparison that takes place in the gateway. Any deviation between divisions that exceeds that established limit will result in an alarm in the MCR.
- Channel functional test is replaced by the periodic calibration verifying the analog modules for drift, the self-monitoring functions ensuring proper functioning of the function processors, and the lack of setpoint drift in a digital system.

The safety-related I&C systems~~PS~~ testing philosophy combines a series of overlapping tests that confirm that the system performs as required. IEEE Std 338-1987 (Reference 8), as endorsed by RG 1.118 (Reference 4), suggests that a single test encompassing each component from the sensor to the actuator is preferable, but allows a series of overlapping tests when a single test is not practical. In the U.S. EPR safety-related I&C systems~~PS~~ design, single functional tests from sensors to actuators are not practical. For example:

07.01-44

components would reduce the reliability of the PS to detect and respond to actual changes in operational conditions.

- Several RT and ESF functions receive input from multiple sensors whose inputs are combined in calculations to determine if the protective function is necessary. For example, the chemical and volume control system (CVCS) isolation on anti-dilution mitigation - standard shutdown conditions function combines inputs from the cold leg temperature (wide range), boron concentration - CVCS charging line, boron temperature - CVCS charging line, and CVCS charging line flow sensors in the calculation of reactor coolant system boron concentration. It is impractical to coordinate simultaneous simulated inputs from multiple sensors in order to determine the operability of the function.
- The RT function on low departure from nucleate boiling ratio (DNBR) receives 173 sensor inputs. It is not possible to design a single functional test from sensor to actuator that would test each combination and permutation of input sensor measurements and verify correct outputs for each case. However, sensor operational tests and calibrations can be performed individually on each of the 173 inputs to verify correct operation of the input channels.

Figure 2-1 represents the U.S. EPR safety-related I&C systems~~PS~~ overlap testing philosophy and shows which portions of the safety-related I&C systems~~PS~~ are periodically tested through technical specification surveillance requirements, and which parts are continuously tested through self-monitoring features.

RAI 505, Question 07.01-44

2.2 *Overlapping Test Coverage*

This section addresses each of the various overlapping tests shown in Figure 2-1, identifies the system equipment covered by each test, and provides information about how the testing is generally performed. Specific testing strategies and procedures will be developed by each COL applicant referencing the U.S. EPR standard design. A COL applicant may choose to perform a surveillance testing alternative from those described in this section. Descriptions of how testing is performed in this section are not intended to constrain a licensee to only these methods. They simply demonstrate that at least one method exists to provide complete, overlapping test coverage of the safety-related I&C systems of the U.S. EPR~~PS~~.

RAI 505, Question 07.01-44

2.2.1 *Calibration*

Calibration refers to the adjustment, as necessary, of a sensor output so that it responds within the necessary range and accuracy to known values of the parameter that the sensor monitors. Calibration includes all devices in the instrument channel required to function for an accurate parameter value to be received by the APU or CU function processor.

In the U.S. EPR PS design, calibration includes the following equipment:

- Sensor.
- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the APU.
- APU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the PS service unit (SU).

In the U.S. EPR SAS design, calibration includes the following equipment:

- Sensor.
- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the CU.
- APU function processor to the extent that the sensor measurement is acquired

RAI 505, Question 07.01-44

by the application software and the value used in the application software is viewed from the SAS service unit (SU).

The method used to perform a calibration depends on the type of sensor being tested. In cases where the sensor is accessible, and suitable test equipment exists (typical pressure and level sensors), a substitute input to the sensor of the same nature as the monitored variable is used. The measurement value acquired by the application software in the function processor is viewed from the respective system's SU to verify accuracy of the measurement channel.

Calibration of resistance temperature detectors (RTDs) is performed by cross checks. During several isothermal plant conditions, the RTD values acquired in the APU or CU function processor application software can be viewed via the respective system's SU. The values of redundant RTD measurement are compared at each of the isothermal conditions to determine an acceptable value. Calibration parameters can then be adjusted in the application software so that each RTD measurement is accurate with respect to the cross calibrated value.

Calibration of analog rod cluster control assembly (RCCA) position measurements is performed by comparing it to the digital RCCA position measurements. The analog position measurement acquired by the application software in the APU function processor can be viewed from the PS SU. This value is compared with the digital RCCA position measurement provided by the reactor control surveillance and limitation system (RCSL~~S~~) to verify consistency within a specified tolerance.

Calibration of self-powered neutron detectors (SPND) is performed based on flux mapping by the aeroball measurement system (AMS). The principles of SPND calibration based on the AMS flux mapping are described in detail in Appendix B of ANP-10287P, "U.S. EPR Incore Trip Setpoint and Transient Methodology" (Reference 13). The resulting SPND calibration factors are entered into the APU function processor application software via the PS SU.

RAI 505, Question 07.01-44

Calibration of boron concentration measurement is performed based on a reference measurement (e.g., chemical analysis of a sample of the fluid in the piping where the boron concentration measurement sensor is located). The boron concentration measurement acquired by the application software in the APU function processor can be viewed from the PS SU. This value is compared with the reference measurement to verify consistency within a specified tolerance.

Calibration of power range detectors is performed based on a power calorimetric and flux map performed at or above 20 percent reactor thermal power. The power range measurement acquired by the application software in the APU function processor can be viewed from the PS SU. The power range measurements are normalized based on the calorimetric and flux map results.

Calibration of intermediate range detectors is performed by obtaining the detector plateau or preamp discriminator curves, evaluating those curves, and comparing the curves with the manufacturer's data. The intermediate range measurement acquired by the application software in the APU function processor can be viewed from the PS SU and adjustments made based on results from comparing the curves with the manufacturer's data.

Calibration of the HMS is performed differently than the previously mentioned devices because the HMS does not interface with the PS or SAS. A substitute input to the sensor of the same nature as the monitored variable is used and the display of this variable is on the SICS and PICS. The measurement value is viewed from the SICS and PICS to verify accuracy of the measurement channel.

2.2.2 *Sensor Operational Test*

A sensor operational test is the injection of a simulated or actual signal into a PS or SAS division as close to the sensor as practicable, and capture of the injected signal when it reaches the application software of the APU or CU function processor. This process

RAI 505,
Question
07.01-44

allows verification of accuracy and response time of devices between the sensor and the APU or CU function processor.

In the U.S. EPR PS design, sensor operational tests include the following equipment:

- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the APU.
- APU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the PS SU.

In the U.S. EPR SAS design, sensor operational tests include the following equipment:

- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the CU.
- CU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the SAS SU.

The method used to perform a sensor operational test is the same for all sensor types. This method consists of injecting a test signal into either the black-box monitoring system or the SCDS, allowing the signal to propagate to the APU or CU function processor, and reading the test signal via the respective system's SU. The test signals are injected via permanently installed test plugs so that no lifting of leads, temporary jumpers, or make-shift connections are required. The use of a ~~portable~~ test ~~computer~~ machine allows injection of a precise test signal and allows precise measurement of the time required for the signal to reach the APU or CU function processor.

RAI 505, Question 07.01-44

Figure 2-2 shows the concept for performing sensor operational tests for sensors that are processed by black box monitoring systems. Figure 2-3 shows the concept for sensors that are not processed by black box monitoring systems. The configuration shown is the bounding case for a sensor being shared by PS and SAS. If the sensor is only used by PS, the SAS CU, MSI and Service Unit are not included as part of this test. If the sensor is only used by SAS, the PS APU, MSI and Service Unit are not included as part of this test.

The sensor operational test of the HMS is performed differently than the previously mentioned devices because the HMS does not interface with the PS or SAS. The sensor operational test of the HMS is performed by injection of a simulated or actual signal into the HMS and the display of this signal on the SICS and PICS. This information will be available to verify the accuracy of the devices between the sensor and the SICS and PICS.

2.2.3 *Setpoint Verification*

Setpoint verification is performed to verify that correct values for nominal trip setpoints reside in the application software of the APU or CU function processor. This verification is performed periodically to protect against human errors that may lead to an incorrect value for a nominal trip setpoint being loaded into the APU or CU.

In the U.S. EPR ~~PS~~ safety-related I&C system design, setpoint verification includes the following equipment:

- The APU function processor to the extent that the nominal trip setpoint value resides in the application software of the APU function processor.
- The CU function processor to the extent that the nominal trip setpoint value resides in the application software of the CU function processor.

The setpoint verification is performed by displaying the setpoint values residing in the APU or CU application software on the respective system's SU, and manually compares

RAI 505, Question 07.01-44

those values with reference values (e.g., those documented in plant setpoint calculations).

2.2.4 *Response Time Tests*

Response time tests are used to verify that the ~~PS~~ safety-related I&C system's actuation response times are less than or equal to the maximum values assumed in the accident analysis. The entire actuation path from sensor to actuator is subject to response time testing. For the reasons cited in Section 2.1, response time testing is performed as a series of overlapping tests that include each component in the actuation path. Response time testing for the SAS is not required in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1.

2.2.4.1 *Sensors*

The response time of the sensor can be tested by providing a substitute input of the same nature as the monitored variable and recording the time the sensor output takes to accurately reflect the substitute input. In many cases, this type of testing is cumbersome and requires removing the sensor from its installed location to perform the testing. ~~Alternatively, a licensee can submit a request to the NRC that justifies excluding sensors from response time testing. In either case, t~~The response time of the sensor must be included in the periodic determination that the overall ~~PS actuation~~ function responds within the maximum time assumed in the plant accident analyses.

RAI 505, Question 07.01-44

2.2.4.2 *Sensor Output to APU Function Processor*

The response time of the equipment between the sensor output and the APU function processor can be verified during performance of the sensor operational tests as described in Section 2.2.2.

2.2.4.3 *APU Inputs to ALU Outputs*

The response time of the equipment comprising the APU, ALU, and communication links between the two is tested using a test input signal, allowing the test signal to propagate through the APU, communication networks and ALU, and acquiring the test signal output from the ALU. Simple logic dedicated to the response time test is included in the application software of the APU and ALU function processors. This means the response time testing can be performed while the PS equipment is actively functioning without impacting the logic that performs the protective functions. The response time of an actuation path can be accurately measured through a dedicated logic path that does not include the protective function logic for the following reasons:

- Binary and analog inputs to a function processor are read once by the function processor at the beginning of each clock cycle.
- Inputs received via data communication messages are read once by the function processor at the beginning of each clock cycle.
- Logical functions in the application software are performed once during each clock cycle.
- Binary or analog outputs are updated once with the results of the logical functions at the end of each clock cycle.
- Output data communication messages are output once at the end of each clock cycle.

This deterministic behavior dictates that the response time is the same for all signals processed by the same function processor and follows the same communication path between function processors.

One method for performing this response time testing is shown in Figure 2-4. A single manual control is used to provide hardwired inputs to APU in each of the four PS divisions. The same control also starts the timer of a test machine. Each APU processes the test signal and sends it via data communication to an ALU in one division, where a two-out-of-four logic is performed on the four test signals. The ALU then provides a dedicated output that is acquired by the test machine and stops the timer. The test is then repeated using the same APU in each division, but acquiring the test output from an ALU in another division. This testing is repeated until each APU-to ALU-actuation path has been tested.

Each function processor and communication module in the PS operates strictly cyclically with a fixed, pre-determined cycle time. They also operate asynchronously from one another. Because of this, while the response time is the same for all signals using the same path, this response time varies. For example, in one instance an input signal could change near the end of a clock cycle and be read-in at the beginning of the next cycle. In another instance the input signal could change just after the beginning of a clock cycle and not read-in until the beginning of the next cycle. These two instances result in two slightly different response times. Due to this effect, each response time test must be performed multiple times, verifying that each test result does not exceed the response time requirements for the system.

2.2.4.4 *ALU Outputs to Actuator*

The response time of the equipment between the ALU output and the actuator can be verified during performance of the actuating device operational tests (ADOT) as described in Section 2.2.5.

2.2.5 *Actuating Device Operational Test*

An ADOT consist of operating the actuating device and verifying the correct operation of each device from the outputs of the PS or SAS to the actuator.

In the U.S. EPR PS design, ADOT includes the following equipment:

- Manual Controls for RT and ESF functions
- ALU function processor to the extent that the application software provides a signal to the output module to simulate an actuation output.
- Output modules of the ALU.
- PACS priority module for engineered safety feature actuation system (ESFAS) initiations.

RAI 505, Question 07.01-44

- Switchgear for ESFAS initiations.
- Plant actuator for ESFAS initiations.
- Trip breakers and trip contactors for RT initiations.

RAI 505, Question 07.01-44

In the U.S. EPR SAS design, ADOT includes the following equipment:

- CU function processor to the extent that the application software provides a signal to the output module to simulate an actuation output.
- Output modules of the CU.
- PACS priority module for engineered safety feature (ESF) control functions.
- Switchgear for ESF control functions.
- Plant actuator for ESF control functions.

Different methods are used to perform ADOT for ~~ESFAS~~ ESF (ESFAS and ESF control) functions and RT functions.

RAI 505, Question 07.01-44

2.2.5.1 *ADOT for ~~ESFAS~~ Actuators Controlled by PS and SAS*

For ~~ESFAS~~ actuators controlled by PS and SAS, two overlapping tests (i.e., no-go test and go test) are used to provide test coverage of each component between the PS and SAS outputs and the actuator. In a no-go test, the PS and SAS ~~outputs are activated~~activation signals are sent ~~(actuation signals are sent)~~ and acquired by the PACS priority module, but the outputs of the priority module are blocked to prevent the actuator from responding. In a go test, the non-safety-related I&C is used to exercise the actuator via the PACS priority module. The ADOT confirms both the functional capability and response time of the equipment between the PS outputs and the actuator. The ADOT confirms the functional capability of the equipment between the SAS outputs and the actuator.

RAI 505, Question 07.01-44

2.2.5.1.1 ~~ESFAS~~ "No-Go" ADOT

RAI 505, Question 07.01-44

Each ~~ESFAS~~ actuator controlled by PS and SAS has a dedicated PACS priority module. For a given ~~ESFAS~~ function, the PS or SAS sends actuation signals to the priority modules corresponding to the actuators required for that function. The no-go test duplicates this functionality by prompting the PS or SAS to send actuation outputs to all priority modules involved in a particular ~~ESFAS~~ function. Priority modules receiving ~~ESFAS~~ signals are tested functionally on a single processor in a single division. A single input function and all related outputs from the processor are verified in a single test. The test is initiated via the respective system's SU and performed by dedicated logic in the ALU or CU application software.

Figure 2-5 shows logic that could be used to perform a no-go test. The example in Figure 2-5 (Sheet 1) is for an ESFAS function that includes three actuators. When the test release parameter has been set to "1," the test is initiated. A dedicated ALU output is generated to block the output of the priority module to prevent the actuator from responding. The blocking signal from the ALU output initiates a 5 second test mode in the priority module of the PACS, where the outputs of the priority module of the PACS are blocked (via a logic AND). If a legitimate protection function is initiated during this 5 second test mode, the outputs of the priority module of the PACS remain blocked. After the 5 seconds, the priority module of the PACS automatically exits the test mode, and the outputs of the priority module ~~become enabled (~~can send actuation signals ~~can be sent)~~. One function of one division of the PS is tested at a time. If a legitimate protection function is initiated ~~-~~during a test, then the other PS divisions will execute the protection function. One second after the test is initiated, the ALU actuation outputs for the ESFAS function ~~are activated (~~send actuation signals ~~are sent)~~ for three seconds ~~and sent~~ to the group of priority modules involved in the function being tested. This results in 1 second between when the priority module of the PACS enters test mode, and the ALU actuation outputs for the ESFAS function are activated. This also results in 1 second between when the ALU actuation outputs for the ESFAS function ~~are deactivated (~~removes its actuation signals ~~are removed)~~, and the priority module of the

PACS exits test mode. This ALU output is acquired by ~~a~~ the test machine, via a permanently installed test connection, to verify that the ALU output is generated and to start a timer. The output of each priority module is also acquired by the test machine, via a permanently installed test connection, to verify that the signal was processed correctly by the priority logic and to stop the timer. In this way, the functionality of the ALU output module, wiring between the ALU and priority module, and the priority logic are verified. The response time of each priority module is also verified.

The primary reason a test machine is needed for this test is to verify the response time of the priority logic. ~~A COL applicant referencing the U.S. EPR standard design may propose to exclude the priority logic from periodic response time testing. This would require the applicant to submit a topical report justifying that approach.~~
~~If the priority logic is excluded from response time testing because there is no response time requirement for this equipment, then the priority logic outputs can be wired to the monitoring service interface (MSI), and the functionality verified via the SU~~. The SAS does not have any response time surveillance requirements, therefore for the ~~ESF control functions'~~ "No-Go" test, the test machine is not utilized. This configuration is shown in Figure 2-5 (Sheet 2).~~If the priority logic is excluded from response time testing because there is no response time requirement for this equipment, then the priority logic outputs can be wired to the monitoring service interface (MSI), and the functionality verified via the SU. The SAS does not have any response time surveillance requirements, therefore for the ESF control functions' "No-Go" test, the test machine is not implemented. This configuration is shown in Figure 2-5 (Sheet 2).~~

RAI 505, Question 07.01-44

RAI 505, Question 07.01-44

The no-go test for SAS ~~the ESF control functions~~ must be performed twice to test both the master and hot-standby CUs in a division. One no-go test will be performed on the master CU, then a manual switchover will occur, and a no-go test will be performed on the new master CU (formerly the hot standby). This test must be done on the master CUs to be able to test the associated PACS priority modules. The switchover is verified via the SAS SU through the SAS MSI.

For certain functions (e.g. CCWS RCP thermal barrier containment isolation valves interlock), an inoperable division may put the system in an undesirable state for normal operation. Therefore, testing procedures are implemented to verify that the valves in the system are in the proper position to ensure continued system operation, before the test is executed. For systems that are fed by two redundant trains, the system is manually aligned to feed from trains that are not under test, while the redundant train is being tested.

RAI 505, Question 07.01-44

2.2.5.1.2 ~~ESFAS~~ "Go" ADOT

The go portion of the ~~ESFAS~~ ADOT overlaps the no-go test in the priority logic of the PACS and includes the switchgear and the actuator itself. The go tests are performed on a per-actuator basis (i.e., each actuator is operated individually). This testing consists of exercising the actuator from the operator's normal human machine interface (HMI) in the main control room (MCR). The operator takes a manual action from the PICS to initiate operation of the actuator. The signal is transferred from the PICS to the PAS and then to the PACS priority logic via the PACS communication module. The priority logic then provides an output to the switchgear, and the actuator responds accordingly. The time stamping capabilities of the PAS are used to capture the time of the actuation output and the time that indication is received that the actuator has responded. The nature of feedback to PAS that the actuator has completed its action depends on the type of actuator and the maintenance procedures used by the plant operator. Typically, limit switches are used to indicate valve actions and either pump speed or flow measurements are used to determine that a pump has achieved its rated speed or flow. In this way, both the functionality and response time of each component downstream of the PACS is verified. Figure 2-6 shows the concept for the go test portion of ADOT.

2.2.5.1.3 ADOT for PS ESF~~AS~~ Outputs to Other I&C Systems

There are three cases where the PS sends an output to another I&C system as part of an ESF~~AS~~ function:

RAI 505, Question 07.01-44

- Partial cooldown output to SAS to control main steam relief control valves.
- Emergency feedwater (EFW) actuation output to SAS to control SG level.
- Output to TG I&C for turbine trip following an RT.

For these three cases, a no-go test is used to verify that the PS output signal is generated and received by either the SAS or TG I&C. This test must be performed twice to test both the master and hot-standby CUs in a division. One no-go test will be performed on the master CU. Then a manual switchover will occur, and a no-go test will be performed on the new master CU (formerly the hot standby). The switchover is verified via the SAS SU through the SAS MSI. Figure 2-5 (Sheet 3) shows the concept for the no-go test for the PS ESF output to SAS functions. For the no-go test for the PS ESF output to TG I&C, the test signal generation is the same with previously discussed no-go tests, but the verification of the signal being received by the TG I&C can be done by plant personnel on the TG I&C service equipment. Plant technical specifications require testing of the outputs from SAS or TG I&C to their respective ESF~~AS~~ actuators.

RAI 505, Question 07.01-44

2.2.5.2 *ADOT for Reactor Trip*

Functional testing of the ALU RT outputs and trip devices (i.e., breakers and contactors) can be performed during plant operation per division. Four divisional RT manual controls are provided to the operator on the SICS. Each of these manual controls is acquired by the ALUs in one PS division, and combined with the automatic RT logic in the application software to generate an RT output. Activation of each manual control results in opening one RT breaker and one fourth of the RT contactors. This does not cause a reactor scram as RT outputs from two PS divisions are required to interrupt power to the RCCAs. Position indications of the trip breakers and contactors are acquired by the PAS and displayed to the operator on PICS to verify that the trip devices have responded to the divisional RT signal.

Rod drop testing is performed during refueling outages in accordance with U.S. EPR Technical Specification, Surveillance Requirement 3.1.4.3. The same manual controls from SICS can be used for this purpose except that all four controls are activated simultaneously to achieve actual RCCA insertion into the core. The response times related to the trip devices and RCCA insertion are measured as part of this testing.

RAI 505, Question 07.01-44

2.2.5.3 *ADOT for Manual Controls*

Functional testing of manual controls consists of initiating the manual control and observing the corresponding feedback. Functional testing of some manual controls (e.g. RCP Trip) may be required only during outages. For manual controls that may be tested at power, one manual control is tested at a time. If a single manual control actuates a component, the feedback is displayed on the PICS. This is similar to the ESF "Go" ADOT except the actuation is initiated in SICS, and the feedback can be observed on PICS or SICS. If a single manual control does not actuate a device (e.g. 2-out-of-4 voting on 4 manual controls) the manual control's signal to the ALU can be read by the PS SU. The SAS has no technical specification surveillance requirements for manual controls.

Manual controls for permissive functions may be tested at power. One manual control can be initiated, when the conditions are not necessary for the permissive to change state. The manual control's signal to the APU can be read by the PS SU.

2.2.6 *Channel Checks*

A channel check is defined in Technical Specifications. A channel check shall be the qualitative assessment, by observation, of channel behavior during operation. This determination shall include, where possible, comparison of the channel indication and status to other indications or status derived from independent instrumentation channels measuring the same parameter.

The automated channel check takes place in the gateway computer that interfaces the input signals in the PS and SAS to the Plant Data Network. The redundant signals from each division are compared periodically in the software to look for deviations between

RAI 505, Question 07.01-39

signals. In addition, the operator shall verify the performance of the automated channel check every 31 days.

RAI 505, Question 07.01-39

~~2.2.6~~2.2.7 *Self-Monitoring Features*

Information contained in this section is generically applicable to TXS microprocessor based systems (applies to both PS and SAS).

Self-monitoring features fall into one of two main categories: Inherent self-monitoring, and engineered self-monitoring. Inherent self-monitoring features are those that are contained in the TXS system software and are present in every TXS system. Engineered self-monitoring features are those that are designed on a project-specific basis as part of the application software.

The inherent and engineered self-monitoring features together provide exhaustive coverage of detecting failures that could prevent performance of a safety function. The coverage of the self-monitoring features is shown in Table 2-5.

~~2.2.6.1~~2.2.7.1 *Software Based Self-Test (Inherent)*

Extensive self-testing is designed as part of the TXS system software. It consists of one part, which is executed once during every startup (i.e., extended self-test), and another part, which is processed repeatedly during operation of the TXS function processor (i.e., continuous self-test). Table 2-1 provides an overview of the self-tests including whether they are executed as part of continuous and/or extended self-testing. Additional self-test features are described in Appendix B.

RAI 505, Question 07.01-44

The continuous self-test performs only those tests which can be performed without affecting the operation of the application software. The continuous self-test is executed repeatedly during the function processor's cyclic processing. It is executed as an operating system task with the lowest priority. Thus, the operating system schedules the continuous self-test only if no other task with higher priority (e.g., the cyclic processing of application software and the processing of service commands) is pending. If the continuous self-test detects an error, it activates the exception-handler to receive error information. The exception-handler (see Section 2.2.6.3) then executes a reset or ends function processor communication by disabling the power supply of the output modules.

Executing each test of the continuous self-test task takes several minutes, the exact amount of time depends on the free time available in each clock cycle after the application processing and the service task. The runtime environment (RTE) monitors the periodic execution of the continuous self-test. If the continuous self-test is not complete after one hour, the runtime environment issues an error message that is stored in a local error message buffer and is also transferred to the SU. This error message is also transferred to the application software for inclusion in engineered alarms to the operator.

When a self-test alarm is received, it is necessary to connect the SU to the faulted function processor to download all error messages to inspect the cause of the alarm. After required information is collected, a reset of the function processor is performed. This reset will initiate extended self-test that must be passed to resume communication with the system. If the module is unable to pass the extended self test, it is replaced. Upon receiving the alarm, the module is considered inoperable until it or a replacement passes extended self-test. Operability of the function processor is assured by the passing of all tests described in Table 2-1. These tests include verification of processor function, application software, operating system, configuration information, and RAM functionality. This shows that the processor is running the correct version of software, has the approved parameters set and can read and write to RAM.

RAI 505, Question 07.01-39

The extended self-test is initiated by resetting the function processor; it is performed as part of the function processor's startup routine. During the extended self-test, additional tests are performed which can not be performed during operation without affecting the processing of the application software. Any errors detected by the extended self-test prevent the function processor from starting its cyclic processing. The function processor does not complete its startup, but instead enters an endless loop allowing for diagnosis using the maintenance laptop. The maintenance laptop connects to the ~~card~~

RAI 505, Question 07.01-44

function processor's front serial interface and communicates only with this single processor while connected. The single function processor is manually rebooted and run in diagnosis state. This processor is not considered operational while the maintenance laptop is connected and in diagnosis state. Once maintenance is finished, the maintenance laptop is disconnected and the function processor is manually reset. The function processor automatically executes an extended self-test during the restart process; and, if there are no errors, then the function processor automatically enters cyclic operation.

~~*2.2.6.1.1*~~*2.2.7.1.1* ***Functions of the TELEPERM XS Maintenance Laptop***

The maintenance laptop connects to the serial interface on the front of a processor. The maintenance laptop is used in situations when the SU is unable to connect to the device under maintenance. It is used to perform the following functions:

1. Initial Software Loading

   The initial software load is made using the TELEPERM XS maintenance laptop, because bootstrap loading of any TELEPERM XS processor is not possible via the TELEPERM XS service unit because access from the service unit is not possible without TELEPERM XS system software, application software, and pre-defined communication links installed. The SVEx processor can load software from this interface only when the processor is in boot load mode, which requires the function processor to be reset to enter and exit this mode. The Maintenance Laptop is also used to configure the communication modules.

2. After Initial Software Loading

   When the initial software load is complete, the m~~M~~aintenance l~~L~~aptop must be used to install software on a new processor ~~board~~ (e.g., after maintenance replacement) or to install system software upgrades. The maintenance laptop can also be used to load application software revisions on a processor ~~boards~~ (e.g., during an outage or if the service unit is not available).

RAI 505, Question 07.01-44

3. Retrieve Diagnostic Failure Information

The m~~M~~aintenance l~~L~~aptop can be used to retrieve diagnostic failure information from the exception ~~-~~handler buffer to diagnose failures. However, this use is not a typical user maintenance activity but may be used during commissioning testing. For situations where the SU may be unable to connect to the device under maintenance, so the maintenance laptop is used for the diagnostic activities. The SVEx processor can perform only the diagnostic functions from this interface with the processor in diagnostic monitor mode, which requires the function processor to be reset to enter and exit this mode. The maintenance laptop cannot access other local software when in diagnostic monitor mode.

~~2.2.6.1.2~~2.2.7.1.2 *TELEPERM XS Maintenance Laptop Software Installation*

The following software is installed on the TELEPERM XS maintenance laptop:

- Linux operating system (may be a different version than the service unit because of the need to match the Linux version to the hardware of the laptop).
- SPACE engineering tool (same version as the service unit).
- Oracle database (may be a different version than the service unit because of the need to match the Linux version to the laptop hardware).
- TELEPERM XS support for Linux (may be a different version than the service unit because of the need to match the Linux version to the laptop).

~~2.2.6.1.3~~2.2.7.1.3 *Maintenance Laptop and Test Machine Access Control*

The administrative controls for the maintenance laptop and test machine provide software and data security protection from unauthorized activities attempting to introduce or use unrecognized software vulnerabilities. The interface can be accessed only by opening the TELEPERM XS cabinet door, which generates a control room alarm. Resetting a TELEPERM XS processor (to enter boot load or diagnostic monitor modes) also generates a control room alarm. The use of the sveload software requires a license dongle.

The maintenance laptop (including the X4.1 interface connection cable) and test machine are controlled in accordance with the plant software and data security plan required by 10 CFR 73.54. The ~~portable~~ test machine is only used for periodic testing and is normally not connected to the system.

RAI 505, Question 07.01-44

Controls for the maintenance laptop include the following:

- Storage in physically secure location when not in use.
- Physical access controls to prevent unauthorized individuals from obtaining access.
- Ability to configure or secure drives and ports to prevent alternate boot methods.
- Prohibit use for general purpose computing.
- User authorization process.
- Ability to modify or configure TELEPERM XS system files in accordance with established configuration control processes.
- Verify that adequate precautions (e.g., patches up-to-date and on demand virus scan) have been taken prior to connecting to the TELEPERM XS system.
- Verify work authorization prior to connecting to the TELEPERM XS system.
- Prevent ability to modify changeable parameters.
- Prevent ability to initiate signal tracing or issue service requests.
- Prevent ability to access the TELEPERM XS RunTime Environment to change modes.
- Prevent ability to change predefined communication channels in TELEPERM XS system via the maintenance laptop.

The test machine only interfaces to the system under test through hard-wired interfaces (24 VDC input and output); therefore, some of the software controls applicable to the maintenance laptop (modifying changeable parameters, issue service request, etc.) are not applicable to the test machine.

Controls for the test machine include the following:

- Storage in physically secure location when not in use.
- Physical access controls to prevent unauthorized individuals from obtaining access.
- Prohibit use for general purpose computing.
- User authorization process.
- Verify that adequate precautions (e.g. patches up-to-date and on demand virus scan) have been taken prior to connecting to the TELEPERM XS system.
- Verify work authorization prior to connecting to the TELEPERM XS system.

~~2.2.6.2~~2.2.7.2 *Hardware Watchdog Timer (Inherent)*

TXS function processors are equipped with a hardware based watchdog timer. The monitoring time of the watchdog is the cycle time of the runtime environment + 110 millisecond (ms). The hardware watchdog timer must be re-triggered by the runtime environment software before its expiration. If the software fails to do so, an error is assumed and a hardwired signal is used to indicate a processor failure, and to switch off the (input/output (I/O) modules' power supply to verify a defined fail-safe behavior of the affected function processor, independently from software based monitoring. Additionally, the exception-handler is activated, initiating a specific response (see S~~s~~ection 2.2.6.3).

The hardware watchdog timer is periodically tested by the cyclic self-test. For this test, a trip of the watchdog is triggered by the self-test task, and the trip is verified on the

RAI 505, Question 07.01-39

associated interrupt signal. The "normal" response to this watchdog-interrupt is blocked for the duration of the test.

RAI 505, Question 07.01-39

~~2.2.6.3~~2.2.7.3 *Exception-Handler (Inherent)*

The exception-~~-~~handler is activated when exceptional situations are encountered during runtime (also in case of a fault detected by the cyclic self-test). After activation, the exception-handler turns off the outputs through driver calls and stops cyclic communication~~deactivates all output boards through driver calls (provides no outputs), and cyclic communication is stopped~~. Self monitoring result information is saved, which includes: exception type, exception number, exception address, memory dump and stack dump.

Depending on the type of fault, the exception-handler either resets or ~~halts~~ the function processor enters a defined fault state and all output signals are set to predetermined safe states. See Technical Report ANP-10309P for information associated with failure states.~~(the processor enters a defined fault state and all output signals are set to predetermined safe states. See Technical Report ANP-10309P for information associated with failure states) the function processor, as indicated~~. If a second exceptional situation occurs within a specified period after a reset (depends on cycle time: e.g., 5 minutes for a 50 ms cycle), the function processor is ~~deactivated~~shutdown. Tables 2-2, 2-3, and 2-4 show the exceptional situations that activate the exception-handler.

RAI 505, Question 07.01-44

~~2.2.6.4~~2.2.7.4 *Error Detection by the Runtime Environment (Inherent)*

[ ]

[ ]

~~2.2.6.5~~2.2.7.5 *Communication Monitoring*

Communication in the TXS system is performed cyclically with a fixed communication cycle time. The communication cycle is the same for all function processors in the system and is specified during the design process. Communication messages are sent once every communication cycle. The receiver performs a series of checks:

- Message header check: Which contains the following information:
  - Protocol version
  - Sender ID
  - Receiver ID
  - Message ID
  - Message type
  - Message length.
- Message age monitoring: The message age is monitored by the runtime environment cycle counter, which is included by the sender in every transferred message. In case one message does not arrive in time, the values of the

message from the previous cycle are allowed to be reused. If for two consecutive communication cycles no new and valid message has been received in time, the signals included in the message are marked with an error status.

[ ]

If one of the listed checks fails, the affected data are marked with an error status. An error message is issued and stored in a local error message buffer and is also transferred to the service unit. These checks are performed by the runtime environment of the function processors. Independently from this, the firmware of the communication ~~processor~~ module performs additional checks (e.g., destination address check, frame check, sequence check). If these checks fail, the received data packet is discarded by the communication module resulting in a loss of the data packet. This loss is then treated by the function processor as previously described (based on message age monitoring).

RAI 505, Question 07.01-44

~~2.2.6.6~~ 2.2.7.6 *Monitoring of the Continuous Self-Test*

The runtime environment monitors the operation of the cyclic self-test. If the cyclic self-test does not complete one self-test cycle within one hour, the runtime environment issues an error message. This does not disrupt runtime environment operation. In particular, the processing of the application software functions is not affected.

2.2.7.7 *Automated Channel Check*

The channel check is a comparison of a parameter on one channel to the parameter on other channels. Significant deviations between two instrument channels could be an indication of excessive instrument drift in one of the divisions, or of something even more serious, such as the failure of an instrument to a high or a low output. A channel check verifies that the instrumentation continues to operate properly between each channel calibration.

The TXS platform is designed to automatically perform the channel check comparisons many times each second. The parameter of each division is compared, for signal deviations, to the other divisional values in the gateway. The limits placed on deviation are based on instrument uncertainty. Analog inputs to TXS are cyclically checked for range violation. Binary inputs to TXS undergo automatic rationality checks. An indication of a fault is alarmed in the MCR.

2.2.7.8 *Automated Channel Function Test Coverage*

The purpose of the channel function test is to confirm that the division is operable. It is a test of the required logic components of each logic path, from as close to the sensor as practicable, up to, but not including, the actuated device.

The DCS is digitally based, and the safety setpoints and logic are set in the software at an exact parameter value for the setpoints. This eliminates setpoint tolerance concerns. This setting does not change over time. The setpoint is permanently set in the software because software does not drift. The channel function test for the new TXS is included in the periodic calibration because the setpoint drift includes the drift of the analog input modules, including analog-to-digital conversion and isolation modules. Since the modules are not adjustable, they are replaced if found out of tolerance during calibration and returned to the manufacturer for repair.

The issues of setpoint setting and instrument drift as they relate to channel function test are not a concern for the processing of safety functions based on digital inputs. The setpoints for digital inputs, where applicable, are set in field sensors that are periodically calibrated to ensure their operability.

The self-monitoring functions confirm proper functioning of the safety function processors, the integrity of the installed code, and provides reasonable assurance of operability ~~and the integrity of the installed code~~. The cyclic self-monitoring routine

RAI 505,
Question
07.01-44

verifies that the code on the FEPROM is the correct version and is not corrupted. The code qualification process has demonstrated acceptability of the code, and the self-monitoring verifies it is an uncorrupted version of the qualified code. The startup test confirms the code stored on the EEPROM in the same manner, prior to reloading the FEPROM. Similarly, the cyclic self-monitoring routine verifies proper functioning of the RAM where the parameter values are stored. The startup test verifies the integrity of the parameter data stored on the EEPROM in the same manner prior to loading the RAM. These tests are equivalent to channel function test verifying that the analog bistable card works electrically and has the correct setpoint.

~~2.2.6.7~~2.2.7.9 *Engineered Self-Monitoring Features*

In addition to the inherent self-monitoring performed by the TXS system software / hardware, additional monitoring is implemented in the application software on a project-specific basis. The engineered monitoring features included in the U.S. EPR design are:

- Monitoring runtime environment message flags to be used in alarm processing.
- Monitoring the signal status of input signals.
- Checking the channel: Analog input measurements received by each safety division are sent to the divisional MSIs and then to the gateways. Within the gateway, signals from redundant divisions are compared for consistency. Inconsistent measurements trigger an indication to the MCR.
- Checking rationality: For example range monitoring of analog input signals or monitoring anti-valent binary input signals. This includes live-zero monitoring for analog signals (i.e., values below 3.5 mA in case of 4-20 mA signals are interpreted as invalid signals, allowing to detect a faulty signal source).

Detection of faults through engineered self-monitoring is then used to:

- Initiate an alarm or indication in the MCR.
- Mark affected signals as faulty and exclude them from further processing.

- Initiate specific measures, such as using a replacement value or triggering/blocking an I&C function (especially in case of multiple faults).

Table 2-2—CPU Exceptions

[ ]

Table 2-5—Self-Monitoring Features Coverage

RAI 505,
Question 07.01-44

Failures detected by inherent features - Failures that are detected by the self-test features as part of the system software (see Table 2-1 for the list of self-tests).

Failures undetected by inherent features - Failures that are not detected by the self-test features as part of the system software (e.g., a temporary fault of RAM cells that is repaired before it is detected by the self-test of the RAM).

Failures detected by engineered features - Failures that are detected by self-monitoring features designed as part of the application software (e.g., channel check or range monitoring).

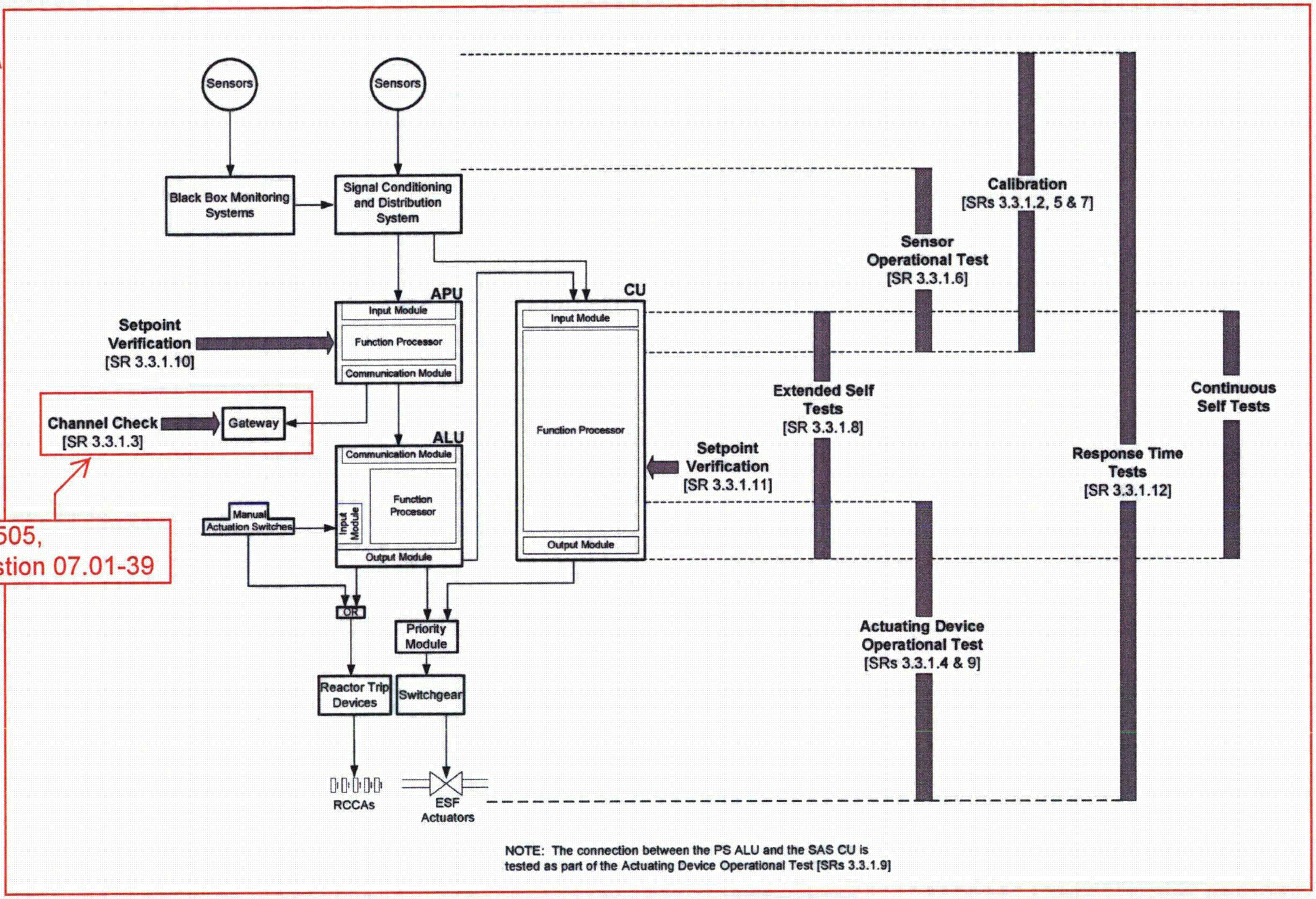
Failures that are non-functional (failure does not prevent proper performance) - Failures that do not prevent the equipment from providing the proper execution of the function (e.g., a failure of the LED on the front plate of the module or a failure of the reset push button on the module).

Failures undetected by inherent features may be detected through engineered features.

If neither the inherent features or the engineered features detects the failure, then the failure is detected through periodic surveillance testing or is a non-functional failure.

RAI 505, Question 07.01-44

Figure 2-1—U.S. EPR PS Testing Philosophy Overview



RAI 505, Question 07.01-39

Figure 2-2—Sensor Operational Testing Including Black Box Monitoring

Figure 2-3—Sensor Operational Testing Excluding Black Box Monitoring

07.01-44

RAI 505,
Question 07.01-44

Figure 2-5 (Sheet 1) — ~~ESFAS~~ "No-Go" Test Concept

RAI 505,
Question 07.01-44

Figure 2-5 (Sheet 2)—~~ESFAS~~ "No-Go" Test Concept

[ ]

RAI 505,
Question 07.01-44

Figure 2-5 (Sheet 3)—~~ESFAS~~ "No-Go" Test Concept

RAI 505,
Question 07.01-44

Figure 2-6—~~ESFAS~~ "Go" Test Concept

d. Providing the actuated equipment with more than one actuation device and testing individually each actuation device.

RAI 505, Question 07.01-44

Conformance:

Testing actuation devices and actuated equipment is performed individually or in judiciously selected groups as described in Sections 2.2.5.1.2, ~~and~~ 2.2.5.2, and 2.2.5.3. In cases where testing the actuated equipment would result in unsafe plant conditions, the actuated equipment is provided with more than one actuation device and the actuation devices are tested individually.

Regulatory Position 3:

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation:

a. Positive means should be provided to prevent expansion of the bypass condition to redundant or diverse systems, and

b. Each bypass condition should be individually and automatically indicated to the reactor operator in the MCR.

Conformance:

Sufficient redundancy is provided in the U.S. EPR PS so performing periodic testing does not prevent the ability of the system to respond to a bona fide accident. Technical Specifications in U.S. EPR FSAR Tier 2, Chapter 16, LCO 3.3.1 verify that all PS functions remain available while the plant is operating in a mode where the functions are required. While bypasses for periodic testing do not prevent the system from performing its function, these bypasses are nonetheless automatically indicated in the MCR on the PICS.

Regulatory Position 4:

Where actuated equipment is not tested during reactor operation, it should be shown that:

a. There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant;

b. The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation, and

c. The actuated equipment can be routinely tested when the reactor is shut down.

Conformance:

In the U.S. EPR design, the only actuated equipment that cannot be tested during reactor operation are those whose operation would adversely affect the safety or operability of the plant (e.g., RCCAs for RT, certain pressure relieving valves). The Technical Specification intervals for surveilling such equipment are based on reliability of the equipment, and support their testing during re-fueling outages. All such equipment can be tested when the reactor is shut down.

3.4 *Regulatory Guide 1.47 "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" [3]*

Regulatory Position 1:

Administrative procedures should be supplemented by a system that automatically indicates at the system level the bypass or deliberately induced inoperability of the protection system and the systems actuated or controlled by the protection system.

Conformance:

Automatic indication of bypasses is provided on the PICS in the MCR. This includes bypasses of ~~PS~~ safety-related I&C system equipment, and bypasses of the systems actuated by the ~~PS~~safety-related I&C systems.

RAI 505, Question 07.01-44

Regulatory Position 2:

The indicating system of Regulatory Position 1 above should also be activated automatically by the bypassing or deliberately induced inoperability of any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system and the systems actuated or controlled by the protection system.

Conformance:

Automatic indication of bypasses is provided on the PICS in the MCR. This includes bypasses of electrical auxiliary support features.

Regulatory Position 3:

Automatic indication in accordance with Regulatory Positions 1 and 2 above should be provided in the control room for each bypass or deliberately induced inoperable status that meets all of the following conditions:

a. Renders inoperable any redundant portion of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety-related functions;

b. Is expected to occur more frequently than once per year; and

c. Is expected to occur when the affected system is normally required to be operable.

Conformance:

Automatic indication of bypasses is provided for the ~~PS~~safety-related I&C systems, the systems actuated by the ~~PS~~safety-related I&C systems, and electrical auxiliary support systems regardless of the expected frequency of bypass occurrences.

RAI 505, Question 07.01-44

Regulatory Position 4:

Manual capability should exist in the control room to activate each system-level indicator provided in accordance with Regulatory Position 1 above.

Conformance:

The PICS in the MCR provides the capability to manually activate each bypass indication.

3.5 *Regulatory Guide 1.118 "Periodic Testing of Electric Power and Protection Systems" [4]*

Regulatory Position:

"Conformance with the requirements of IEEE Std. 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," provides a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to periodic testing of electric power and protection systems if the following exceptions are complied with"

Conformance:

Conformance to this regulatory position is satisfied by U.S. EPR PS conformance to IEEE Std 338-1987 as described in Section 3.8. The exceptions noted in the regulatory position are taken into account in Section 3.8.

3.6 *NUREG-0800, BTP 7-17 "Guidance on Self-Test and Surveillance Test Provisions" [6]*

Acceptance Criteria:

Surveillance test and self-test features for digital computer-based protection systems should conform to the guidance of Regulatory Guide 1.22 and Regulatory Guide 1.118. Bypasses necessary to enable testing should conform to the guidance of Regulatory Guide 1.47.

Conformance:

U.S. EPR PS conformance to RGs 1.22, 1.47 and 1.118 is described in Sections 3.3, 3.4 and 3.5, respectively.

U.S. EPR SAS conformance to RG 1.47 is described in Section 3.4.

Acceptance Criteria:

Failures detected by hardware, software, and surveillance testing should be consistent with the failure detectability assumptions of the single-failure analysis and the failure modes and effects analysis.

Conformance:

The system-level PS failure modes and effects analysis (FMEA) is contained in Reference 11. The system-level SAS FMEA is contained in U.S. EPR FSAR Tier 2, Section 7.1. The system-level analysis assumes that there are no failures that cannot be detected by either surveillance testing or self-testing. U.S. EPR FSAR Tier 1 for safety-related I&C~~,~~ ~~Section 2.4.1~~ contains ITAAC commitments to perform an~~n~~ ~~additional~~ FMEA at the replaceable component level to validate the failure assumptions of the system-level FMEA. This assumption is consistent with the complete testing coverage described throughout this report.

RAI 505, Question 07.01-44

Acceptance Criteria:

Digital computer-based I&C systems should include self-test features to confirm computer system operation on system initialization.

Digital computer-based I&C systems should generally include continuous self-testing. Some small, stand-alone, embedded digital computers may not need self-testing. Typical self-tests include monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

RAI 505, Question 07.01-44

Conformance:

Each PS and SAS function processor is subjected to an extended self-test which is automatically performed on each instance of processor initialization. The extended self-test is described in Section 2.2.6.1.

The PS ~~design contains~~ and SAS designs contain extensive self-testing that is performed continuously (every clock cycle). These self-testing features are described in Sections 2.2.6.1 through 2.2.6.5.

The software for both the self-test and the extended self-test are loaded onto the FEPROM as part of the system segment software. The 2 tests are validated versions from factory testing and their CRC sums are checked every self-testing cycle to assure that they have not been corrupted. Between the qualification of the self-test software at the factory and the periodic checking for no corruption, the ongoing validity of the two tests is verified. If the CRC check fails the processor reboots, checks it again, and if it fails again the processor shuts down. In the event that this happens, the operator will receive an alarm.

RAI 505, Question 07.01-39

Acceptance Criteria:

The design of automatic self-test features should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. The scope and extent of interfaces between software that performs protection functions and software for other functions such as self-test should be designed to minimize the complexity of the software logic and data structures. The safety classification of the hardware and software used to perform automatic self-testing should be equivalent to the tested system unless physical, electrical, and communications independence are maintained such that no failure of the test function can inhibit the performance of the safety function.

Conformance:

RAI 505, Question 07.01-44

The TXS self test features are designed as an integral part of the system software of each PS and SAS function processor. As such, these features are classified as safety-related and are designed and qualified to safety-related standards. Self-tests are performed separately within each PS and SAS function processor and, therefore, have no impact on independence between redundant divisions or on the system's ability to withstand single failures. Self-testing has no impact on the ability of each function processor to perform its safety function as the self-tests are executed at the end of each clock cycle after the processor has finished processing its application software (except in case the self-test detects a fault and resets or shuts down the processor, which is the desired behavior).

Acceptance Criteria:

The positive aspects of self-test features should not be compromised by the additional complexity that may be added to the safety system by the self-test features. The improved ability to detect failures provided by the self-test features should outweigh the increased probability of failure associated with the self-test feature.

Conformance:

The TXS self-test features are designed as an integral part of the system software of each function processor, which minimizes the complexity associated with the inclusion of these features. The assignment of the self-test routines as the lowest priority activity of the processor and their performance only at the end of each clock cycle minimizes the potential for failures associated with the self-test feature.

Acceptance Criteria:

Self-test functions should be verified during periodic functional tests.

Conformance:

Self-test functionality is not directly tested via periodic functional testing. To do so would require injection of faults into the safety system; which is neither prudent nor necessary. It is not prudent because it risks permanent damage to the safety system that may prevent correct functioning in the future, and because it would be difficult to determine that the injected fault had been completely "removed" from the system following the testing. It is not necessary because reasonable assurance of correct self-test operation is provided via other means:

RAI 505, Question 07.01-44

- Indirect periodic testing: The PS and SAS function processors and communication paths are exercised as part of other surveillance testing as described in Sections 2.2.1 through 2.2.5. This verifies that faults resulting in the inability of the equipment to perform its safety function would be detected. Such faults should be detected by self-tests and, if such a fault is detected during other surveillance testing, then incorrect operation of the self-test features are also detected.
- Self-test qualification and configuration control: The TXS system software, including the software used in the self-test process, is developed and tested using a quality program as described in EMF-2110(NP)(A), "TELEPERM XS: A Digital Reactor Protection System," (Reference 10). This verifies that the self-

test features function properly. TXS system software contains an identification file providing a CRC checksum for all files which are delivered within a package (e.g., executable programs, dynamic-link libraries, object modules, pre-links, header files). The CRC checksum of the complete TXS system software installation forms a unique identification of the version. When the TXS system software is loaded onto the TXS processing unit, the CRC checksum of the loaded TXS system software on the TXS processing unit is manually verified to match the CRC checksum of the originally developed and tested TXS system software. This verifies that the system software containing self-test features is identical to that which was tested and verified to operate correctly.

- Continuous monitoring of the self-test: Two mechanisms are used to continuously monitor correct operation of the self-test: the hardwire watchdog timer and the runtime environment. The hardware watchdog timer (described in Section 2.2.6.2) will trip if a failure in the self-test features causes a stop of the function processors cyclic operation. The runtime environment initiates an alarm if the complete set of self-test routines is not completed within one hour.
- Periodic extended self-test: The periodic initiation of the extended self-test includes checks of the memory containing the cyclic self-test software, and a CRC check to verify that both the inherent and engineered software containing the self-test routines is identical to the routines initially loaded onto the function processor.

Acceptance Criteria:

Systems should be able to conduct periodic surveillance testing consistent with the technical specifications and plant procedures. As delineated in Regulatory Guide 1.118, periodic testing consists of functional tests and checks, calibration verification, and time response measurements.

Conformance:

Sections 2.2.1 through 2.2.6 describe how the ~~PS~~ safety-related I&C systems~~is~~ are designed to conduct periodic surveillance testing consistent with technical specifications. Conformance with RG 1.118 via conformance with IEEE Std 338-1987 is addressed in Section 3.8.

RAI 505, Question 07.01-44

Acceptance Criteria:

As required by IEEE Std 279-1971, Clause 4.13, or IEEE Std 603-1991, Clause 5.8.3, and as stated in Regulatory Guide 1.47, if the protective action of some part of a protection or safety system is bypassed or deliberately rendered inoperative for testing, that fact should be continuously indicated in the control room. Provisions should also be made to allow operations staff to confirm that the system has been properly returned to service.

Conformance:

Conformance to guidance relative to bypassed/inoperable status indication is described in Section 3.4.

Acceptance Criteria:

Regulatory Guide 1.118 states in part that test procedures for periodic tests should not require makeshift test setups. For digital computer-based systems, makeshift test setups, including temporary modification of code or data that must be appropriately removed to restore the system to service, should be avoided.

Conformance:

As described in Sections 2.2.1 through 2.2.5, any temporary connections used for surveillance testing are made using permanently installed test connections. Temporary modification of data, in the form of changeable parameters, is used in certain surveillance tests (see Section 2.2.5.1.1). If the parameter is not changed back following testing, it does not prevent the PS or SAS function processor from performing its function. This is verified by the "pulse" function shown in Figure 2-5. Plant post-maintenance testing procedures will include verification that the changeable parameter is changed back to its proper state following surveillance testing.

Acceptance Criteria:

If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic tests during plant operation. The capability to periodically test and calibrate the automatic test equipment should also be provided. The balance of surveillance and test functions not performed by the automatic test feature should be performed manually to meet the intent of Regulatory Guide 1.118. In addition, the automatic test feature function should conform to the same requirements and considerations (e.g., test interval) as the manual function.

Conformance:

There are no automatic test features using automatic test equipment credited to perform surveillance testing in the U.S. EPR ~~PS~~ safety-related I&C systems design.

RAI 505, Question 07.01-44

Acceptance Criteria:

The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system. The design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. Commercial digital computer-based equipment used to perform periodic testing should be appropriately qualified for its function.

Conformance:

The TXS self test features are designed as an integral part of the system software of each PS and SAS function processor. As such it is designed and qualified to safety-related standards. External test equipment used to perform surveillance testing (e.g., SU, test machines) does not perform any safety-related functions and is not required to be designed to safety-related standards. Such equipment is designed and implemented under the TXS quality assurance program as described in Reference 10. The quality assurance program uses a graded approach to quality to verify that digital computer-based equipment used to perform periodic testing is appropriately qualified for its function.

Acceptance Criteria:

The design should have either the automatic or manual capability to take compensatory action on detection of failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures will be consistent with each other.

Plant procedures will specify manual compensatory actions and mechanisms for recovery from automatic compensatory actions.

Mechanisms for operator notification of detected failures will comply with the system status indication provisions of IEEE Std 603-1991 and will be consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures.

Conformance:

RAI 505, Question 07.01-44

Any failed component in the ~~PS~~ safety-related I&C systems design can be removed from service consistent with the prescribed actions in the U.S. EPR Technical Specifications. Plant procedures are outside the scope of this report. Conformance to guidance relative to inoperable status displays are described in Section 3.4.

3.7 *IEEE Std 603-1998 [7]*

The design of U.S. EPR I&C systems complies with IEEE Std 603-1998 in lieu of IEEE Std 603-1991 based on an alternative request pursuant to 10 CFR 50.55a(a)(3)(i).

Clause 5.7 “Capability for Testing and Calibration”:

Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class IE systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

- Appropriate justification shall be provided (e.g., demonstration that no practical design exists),
- Acceptable reliability of equipment operation shall be otherwise demonstrated, and
- The capability shall be provided while the generating station is shut down.

RAI 505, Question 07.01-44

Compliance:

The capability for testing and calibrating the ~~PS~~ safety-related I&C systems is described throughout this report. Plant technical specifications provide appropriate controls to verify that the capability of the ~~PS~~ safety-related I&C systems to perform ~~its~~ their safety functions is retained during testing and calibration. Conformance to IEEE Std 338-1987 is addressed in Section 3.8. Exceptions to testing actuated equipment during plant operation are addressed in Section 2.1.

Clause 5.8.3 “Indication of Bypasses”:

If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

a.) This display instrumentation need not be part of the safety systems.

b.) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable.

c.) The capability shall exist in the control room to manually activate this display indication.

Compliance:

Conformance to RG 1.47 relative to bypassed/inoperable status displays ~~are~~ is described in Section 3.4.

RAI 505, Question 07.01-44

Clause 6.5.1 "Checking the Operational Availability"

Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

a.) By perturbing the monitored variable,

b.) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or

c.) By cross-checking between channels that bear a known relationship to each other and that have readouts available.

Compliance:

The operational availability of each ~~PS~~ safety-related I&C systems input sensor is provided during reactor operation. Sensor calibration and sensor operational tests are described in Sections 2.2.1 and 2.2.2.

RAI 505, Question 07.01-44

3.8 *IEEE Std 338-1987 [8]*

IEEE Std 338-1987 contains sections for design requirements and testing program requirements. The design requirements are addressed in this section. Testing program requirements are not addressed as the testing program employed by a licensee referencing the U.S. EPR Design Certification is outside the scope of this report.

Design Guidance:

(1) Design shall provide the capability for periodic surveillance testing that simulates, as closely as practicable, the required safety function performance.

Conformance:

The U.S. EPR safety-related I&C systems~~PS~~ provide~~s~~ the capability for periodic surveillance testing to the extent required to provide reasonable assurance that the systems will reliably perform their~~its~~ safety functions. This testing capability is described in Sections 2.2.1 through 2.2.5.

Design Guidance:

(2) Test equipment interfaces and installed test equipment shall not cause a loss of independence between redundant channels or load groups.

Conformance:

Test equipment interfaces are provided via appropriate isolation devices as described in Sections 2.2.1 through 2.2.5. Generally, testing is performed on only one redundant portion of the PS or SAS at a time. The exception is response time testing. As shown in Figure 2-4, isolation is provided between redundant PS divisions during response time testing.

07.01-44

Design Guidance:

(3) Safety systems should be designed with due consideration of the impact of testing on plant availability, maintainability, operation, operational mode, and limiting conditions for operation. Coincidence logic may be provided where necessary to fulfill this provision.

Conformance:

Redundancy and coincidence voting logic are provided in the PS and SAS designs to accommodate plant availability, maintainability, operation, and limiting conditions for operation.

07.01-44

Design Guidance:

(4) Testability shall be considered in the selection of all components of the safety system. Sensors should be accessible and, where practicable, installed such that their calibration can be verified in place. When selecting actuation devices, their status indication capability shall be considered.

07.01-44

Conformance:

The TXS platform has been selected for use in the U.S. EPR PS and SAS. The TXS platform provides extensive self-testing capability and modular design that is flexible to allow for appropriate periodic surveillance testing. Selection of other components of the safety system (e.g., sensors and actuation devices) is outside the scope of this report.

Design Guidance:

(5) Design shall provide for the functional testing capability of the safety system. Simultaneous testing of the system from sensor to actuated equipment is the preferred method. However, where this is not practical, the system design shall provide overlap testing capability.

Conformance:

Section 2.1 describes the impracticality of simultaneous testing of the ~~PS~~ safety-related I&C systems from sensor to actuated equipment, and identifies the overlap testing capability that is provided in lieu of simultaneous testing of the systems.

07.01-44

Design Guidance:

(6) Interrelationship among the systems, components, and human factors in each phase of the test activity should be considered and reflected in the system design. Test points, test devices, and associated test equipment should be located to facilitate performance of periodic surveillance testing.

Conformance:

Conformance with this aspect of testing is outside the scope of this report.

Design Guidance:

(7) A means of communication shall be provided between personnel associated with the test and the MCR to ensure that control room operators and associated test personnel are cognizant of the status of those systems under test. In addition, a means of communication shall be provided so that personnel associated with the test can adequately communicate.

Conformance:

Conformance with this aspect of testing is outside the scope of this report.

Design Guidance:

(8) Automatic testing features should be considered when selecting the type of testing system. However, where a programmable digital computer is included in the design, whether integrated or portable, automatic testing features are subject to the provisions of this standard and IEEE Std 7-4.3.2-1982.

Conformance:

Extensive self-test features are included in the PS and SAS designs and are addressed in this report. Conformance to the applicable standards are addressed for the self-tests throughout Section 3 of the report.

Design Guidance:

(9) Design considerations for testing the electrical power, instrumentation, and controls portion of the safety system shall be coordinated with the testing provisions of associated mechanical and fluid systems.

Conformance:

Testing electrical power systems is outside the scope of this report, however sufficient redundancy is provided in the safety-related I&C systems~~PS~~ design to accommodate testing of systems that provide electrical power to the safety-related I&C systems~~PS~~. Sections 2.2.1 and 2.2.2 address the measures included in the design to accommodate testing provisions of instrumentation. Section 2.2.5.1.1 addresses the measures included in the design to accommodate testing provisions of ESF~~AS~~ mechanical and fluid systems.

07.01-44

Design Guidance:

(10) Provisions used for perturbing the same or a substitute process variable are preferred over using simulated signals to verify overall tripping of each protective channel. Where perturbing the monitored variable or substitute is not practical, the proposed alternative tests shall have documented justification.

Conformance:

07.01-44

Tripping of each protective channel is not required by U.S. EPR Plant Technical Specifications, and is not necessary as a result of using a software based digital PS and SAS. The purpose of this type of test in analog ~~PSs~~ protection systems was to detect and correct drift that occurred in the bi-stable setpoint devices. Software-based setpoints do not experience drift. In the U.S. EPR design, a combination of sensor operational tests and calibration are used to detect and correct drift in the input channels. A combination of setpoint verification and self-testing is used to verify that the setpoints contained in the PS and SAS software are valid.

Design Guidance:

(11) Means should be included in the design to facilitate response time testing from sensor input to, and including, the actuated equipment if required by Clause 6.3.4.

Conformance:

Means are provided in the PS design to facilitate response time testing from sensor to actuator. Section 2.2.4 describes the PS response time testing.

Design Guidance:

(12) Where practical, test devices, such as test blocks, should be incorporated into the design to eliminate the application and removal of wires in order to perform periodic surveillance testing. These devices shall not interfere with the operability or safety function of the component or system under test.

Conformance:

Where temporary connections are used for testing, permanently installed test connections are provided in the design. These test connections do not interfere with the operability or safety function of the safety-related I&C systems~~PS~~. The test descriptions in Sections 2.2.1 through 2.2.5 identify when a permanently installed test connection is used.

Design Guidance:

(13) Where practical, means shall be included in the design to prevent the simultaneous application of any bypass condition to redundant channels or load groups during testing.

Conformance:

In the PS and SAS design, ~~the~~ a SU is used to place equipment in maintenance bypass for testing. The PS or SAS SU can only be connected to one PS or SAS division at a time.

Design Guidance:

(14) Where redundant components are used within a single channel or load group, the design should permit each component to be tested independently.

Conformance:

In the PS design, redundant ALUs exist within each division. Response time testing and no-go actuating device operational tests can be performed on each ALU individually. In the SAS design, redundant CUs exist within each division. No-go actuating device operational tests can be performed on each CU individually.

07.01-44

Design Guidance:

(15) The system should be designed such that the removal of fuses or opening of breakers is only required for the purposes of testing if such action causes the actuation of the logic for a channel or load group. For example, the actuation of' a loss of channel power supply is simulated by the removal of its fuses.

Conformance:

The surveillance tests described in this report do not require removing fuses or opening breakers. Testing of electrical power supply systems is outside the scope of this report.

07.01-44

Sections 2.2.1 through 2.2.6 describe the testing and calibration functions included in the ~~PS~~ safety-related I&C systems design. Performance of these functions does not prevent the safety-related I&C systems~~PS~~ from performing ~~its~~ their safety function. The TXS self-test features are designed as an integral part of the system software of each PS and SAS function processor. As such, it is designed and qualified to safety-related standards. External test equipment used to perform surveillance testing (e.g., SU, test machines) does not perform any safety-related functions and is not required to be designed to safety-related standards. Such equipment is designed and implemented under the TXS quality assurance program as described in Reference 10. The quality assurance program uses a graded approach to quality to provide reasonable assurance that digital computer-based equipment used to perform periodic testing is appropriately qualified for its function.

Clause 5.5.3 "Fault Detection and Self-Diagnostics":

The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.

If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function.

When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

a) Self-diagnostics during computer system startup

b) Periodic self-diagnostics while the computer system is operating

c) Self-diagnostic test failure reporting

Conformance:

The high reliability of the TXS platform is verified by the inclusion of self-test features in the platform design. The self-test features are designed as an integral part of the PS and SAS system software and, as such, are subject to the same safety-related V&V requirements as the rest of the system software. The assignment of the self-test routines as the lowest priority activity of the processor and their performance only at the end of each clock cycle minimize potential for failures associated with the self-test feature. Self-tests are performed during processor startup, continuously during operation, and report detected failures as described in Section 2.2.6.

07.01-44

APPENDIX A
DIVERSE ACTUATION SYSTEM TESTING

A.1 INTRODUCTION

The diverse actuation system (DAS) is periodically tested to verify that the system will execute its functions. Technical specifications require that these tests are performed every 24 months. Most of the functions are capable of being tested with the plant at power. The testing of some functions at power would upset plant operation or damage equipment. For these functions, the tests can be performed when the reactor is in shutdown mode. The DAS testing philosophy combines a series of overlapping tests that confirm the system performs as required:

- Sensor Operational Test – verifies operability of the sensor channel.
- Calibration – verifies the range and accuracy of the sensor channel.
- Actuation Logic Test – verifies operability of logic circuits and accuracy of the desired output.
- Actuation Device Operation Test – verifies that final actuation devices function properly in response to an actuation signal.

RAI 505, Question 07.01-44

- Response Time Test - verifies that actuation response times are less than or equal to the maximum values assumed in the Diversity and Defense-in-Depth assessment.

Figure A-1 represents the U.S. EPR DAS overlapping test philosophy, and shows which portions of the DAS are periodically tested to meet the surveillance requirements. This figure also shows the general concept for each test. Sensors shared by the protection system (PS) and DAS are tested as part of the PS. These sensors are not tested separately as part of the DAS periodic testing.

Functional testing of manual, system-level controls, consists of initiating the manual control and observing the corresponding feedback. The following manual, system-level actuations are also available to the operator on SICS:

- EFW Actuation.
- Medium Head Safety Injection (MHSI) Initiation.
- Stage 1 Containment Isolation.
- Containment Hydrogen Mixing Dampers Opening.

Activation of each manual control results in actuation orders for multiple pumps and/or valves. The actuation orders are sent to the PACS modules for the individual components. Limit switches are used to indicate valve actions, and either pump speed or flow measurements are used to determine that a pump has achieved its rated speed or flow. These sensors are acquired by the SCDS, processed by PAS, and displayed to the operator on PICS to verify that the individual components have responded to the manual, system-level actuation order. Functional testing of these manual controls at power would upset plant operation or damage equipment, so these tests are performed when the reactor is in shutdown mode.

RESPONSE TIME TESTING

Response time tests are used to verify that the actuation response times are less than or equal to the maximum values assumed in the diversity and defense-in-depth assessment. The entire actuation path from sensor to actuator is subject to response time testing. The testing is performed as a series of overlapping tests that include each component in the actuation path.

The response time of the sensor can be tested by providing a substitute input of the same nature of the monitored variable and recording the time the sensor output takes to accurately reflect the substitute input. In many cases, this type of testing is cumbersome and requires removing the sensor from its installed location to perform the testing. The response time of the sensor must be included in the periodic determination

RAI 505,
Question 07.01-44

that the overall function responds within the maximum time assumed in the diversity and defense-in-depth assessment.

The response time of the equipment between the sensor output and the setpoint comparison logic of the DAS can be verified during performance of the Sensor Operational Tests.

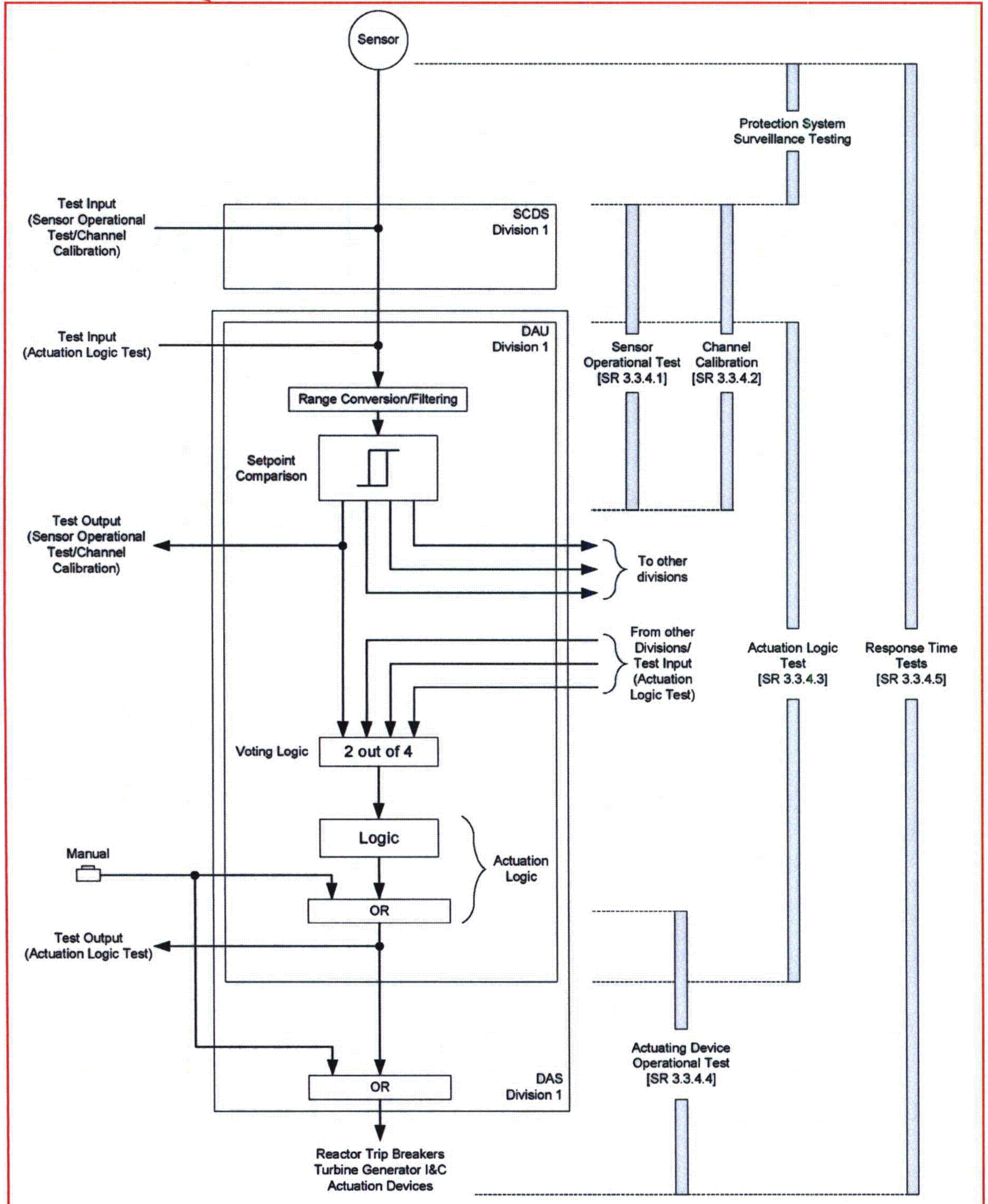
The response time of the equipment comprising the DAU can be verified during performance of the Actuation Logic Test.

The response time of the equipment between the actuation logic of the DAU and the actuator can be verified during performance of the Actuating Device Operational Test.

RAI 505,
Question 07.01-44

RAI 505,
Question 07.01-44

Figure A-1—DAS Testing



APPENDIX C
PACS LOSS OF POWER TESTING

[ ]