

SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.: 356-7881
Review Section: 07 – Instrumentation and Controls – Overview of Review Process
Application Section: 7.0
Date of RAI Issue: 01/04/2016

Question No. 07-3

Describe the diagnostic programs used to test digital computer channels in the APR1400 design.

As required by 10 CFR 50.55a(h)(3), IEEE Std. 603-1991, Clause 5.7, states, in part, that 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. APR1400 FSAR Tier 2, Chapter 16, Section 1.1, "Definitions" states with regard to the Channel Functional Test, in part,

"Digital Computer channels - the use of diagnostic programs to test digital computer hardware and the injection of simulated process data into the channel to verify OPERABILITY, including alarms and trip functions."

1. Describe the diagnostic programs used for testing. Specifically, what are these programs? How do they help to ensure operability of safety system components?
2. Describe the testing process or describe where in the application the testing process is explained in detail.
3. How does the design ensure that there is adequate independence such that injected signals are only received by the channel being tested and not to other channels on the safety system data network?
4. How does the design ensure that online testing does not result in an unplanned component or spurious actuation of a component(s) while testing is being performed?

Response

1. The diagnostic programs used to monitor the integrity of the hardware are addressed in the response to RAI 356-7881 Question No. 07-1. This consists of the automatic self-test functions provided by the AC160 module self-diagnostics and the application automatic self-checking features which are discussed in the response to both RAI 356-7881 Question No. 07-1 and 07-2.

Surveillance testing provisions for the reactor protection system (RPS) are provided by the set of overlap tests depicted in Figure 7.2-11, "PPS Testing Overlap" of DCD Tier 2 and Figure 4-6, "Overlap in Functional Testing for the PPS" of the Safety I&C System technical report.

The starting point of a test, as depicted in the figures identifies the entry point in the signal path where a test signal specified by the maintenance and test panel (MTP) is injected into the signal path. The endpoint of a test depicts the point in the signal path where monitoring signals representing the results of system processing are provided, which can be observed on the MTP flat panel display (FPD).

Surveillance testing provisions for the engineered safety features (ESF) are provided by a combination of the overlap tests identified in Figure 7.2-11 of DCD Tier 2 and the test logic depicted in Figure 7.3-22, "ESF-CCS Simplified Test Logic Diagram" (to cover the signal path through the engineered safety features – component control system (ESF-CCS) group controllers) of DCD Tier 2.

Operation of the overlap tests identified in Figure 7.2-11 of DCD Tier 2 is accomplished by observation/comparison of the redundant process inputs to the PPS from each channel, replacement of the actual inputs or intermediate calculations with test signals which follow the same signal path as the input or calculated signals, and observation of the results of the system processing associated with the injected test signals.

Operation of the test logic depicted in Figure 7.3-22 of DCD Tier 2 is accomplished by injection of test signals into the normal signal path of the ESF-CCS group controllers and observation of monitoring points provided to the MTP FPD.

Therefore, the proper operation of the safety system components is assured by a combination of:

- No diagnostic error messages (hardware operating properly),
- No CRC changes on the AC160 processor modules (software has not changed)
- The injected test signals utilize the same path as actual signals (tests actual logic)
- The monitored response is the expected response (logic is correct)

This approach is described and approved in the Common Qualified Platform Topical Report.

2. Section 4.2.2.2, "Manual Testing Features" of the Safety I&C System technical report provides the specific tests that can be initiated and performed during plant power operation as well as during plant shut down. These tests are initiated from the MTP FPD over division paths that range from sensor inputs to the reactor trip switchgear system (RTSS) or the input of the ESF-CCS as shown in Figure 4-6, "Overlap in Functional Testing for the PPS" of the Safety I&C System technical report. Also, Section 7.2.2.5 of DCD Tier 2 provides descriptions of the specific types of tests used to verify the integrity of the PPS and the CPCS and the trip path from the sensor input to the reactor trip switchgear. As shown in Figure 7.2-11, "PPS Testing Overlap" of DCD Tier 2, the PPS test is performed over the overlap test area to verify the functionality of the entire PPS.

Operation of these tests is accomplished by observation of redundant process sensor inputs from each channel on the MTP FPD, injection of MTP specified test signals into the PPS signal path, and observation of monitoring points provided on the MTP FPD.

3. The MTP and interface and test processor (ITP) are used to support the periodic testing of the safety I&C system. Tests are initiated from the MTP FPD. The test injection signals are provided by the MTP or ITP, and the tests provide monitoring points (i.e. test feedback) that can be displayed on the MTP FPD. Sections 7.2.2.5 and 7.3.2.5 of DCD Tier 2 state that the test equipment consists of divisionalized MTP, ITP, and the associated interface circuits.

The safety system data network (SDN) is used to communicate test injection signals and monitoring points (i.e. test feedback). Section 4.6.2.2 of the Safety I&C System technical report states that the SDN is contained within a division and does not cross safety division boundaries. The architectural design of the SDN does not provide for cross-division communication. Therefore, test injection signals transmitted by the MTP or ITP cannot be received by a process station in a different channel than the transmitting MTP or ITP.

4. Testing during plant power operation is performed through the periodic functional test, which is administratively controlled in accordance with the Technical Specifications.

As described in Section 7.2.2.5 of DCD Tier 2, the system test does not affect the protective functions and meets the guidance of IEEE Std. 338, which is endorsed by NRC RG 1.118. The testing also complies with RG 1.22. In addition, Section 3.2, item j. of the Safety I&C System technical report provides analysis regarding GDC 21, "Protection System Reliability and Testability."

The channel bypass is required to be applied to the trip parameter(s) to be tested in a channel which is undergoing testing. This procedure prevents any safety related components or devices from operating in an unintended way due to the test signals.

Supplemental Response

There are several provisions in the APR1400 design to ensure that there are no unintentional equipment actuations as a result of testing a single channel or multiple channels. As provided in response to sub-question 3 above, DCD Tier 2 Section 7.2.2.5 states that the test equipment consists of divisionalized MTP, ITP, and the associated interface circuits. The simulated test signals only affect the channel under test and therefore there is no chance for the test signals to be transmitted to other channels. Additionally, the operator must go through multiple secured steps for initiating tests, such as enabling the function enable switch, going into the correct testing display of the MTP, and pressing the correct testing request from the MTP FPD.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

There is no impact on any Technical, Topical or Environmental Report.