Questions and Answers for Chapter 7 related Conference Call

Please see the specific issues we would like clarification on described below. Please be advised that some of this information is proprietary.

1. Section A.5.7 of the Technical Report, APR1400-Z-J-EC-13001-P, “Safety I&C System for the APR1400” states that the safety I&C system incorporates enhanced continuous system self-checking features that minimize required manual surveillance and periodic testing and reduces the likelihood of undetected failures. Based on this statement, it seems that self-testing features are being credited to minimize manual Tech Spec surveillance requirements. However, based on discussions with the NRC reviewers from the Tech Specs branch, this is not something that was mentioned in the Tech Specs or the Tech Specs basis. We would like to get confirmation from KHNP on whether self-testing features are being credited to minimize manual Tech Spec surveillance requirements.

   Response

   As stated at the 7th PARM held on July 2012, the manual periodic surveillance testing is performed according to the Technical Specifications. The manual testing covers all trip signal paths from the sensor input to the actuation devices as described in Section 7.2.2.5 and Figure 7.2-11 “PPS testing overlap” in the DCD Tier 2.
   Tech Spec surveillance requirements do not credit any self-testing features.

2. Section 8 of the Technical Report, APR1400-Z-J-EC-13001-P, “Safety I&C System for the APR1400” discusses the commercial grade dedication plan for the APR-1400 I&C safety systems. This section states that “the safety I&C system, implemented on a common PLC platform, and any safety-related components are qualified to commercial grade dedication (CGD) if they are not manufactured in accordance with 10 CFR 50 Appendix B.” The staff was not able to locate a list of components that are going to be manufactured in accordance to 10 CFR Appendix B and thus the staff is not able to determine which components will be CGD’d. Also, this section states that “in the preliminary phase, the risks and hazards are evaluated, the safety function are identified, configuration management is established, and the safety category of the system is determined. Following the preliminary phase, the commercial grade item is evaluated for acceptability using detailed acceptance criteria. The critical characteristics are identified by a technical evaluation and each critical characteristic is verified by inspection, analysis, demonstration, or testing for three categories of critical characteristics.” It is unclear to the staff when the preliminary phase and the follow phase of this process will be completed (e.g. during the design certification application). In addition, does KHNP have the list of critical characteristics of the CGD’d components or does KHNP only have the categories of critical characteristics established?

   Response

   The CGD plan including the category of critical characteristics has been included in Section 8 of Safety I&C System TeR. Specific components for CGD are not defined at this time, since APR1400 has opted for “platform-neutral” approach.

The first choice will be “Common-Q” which has already been commercially dedicated, and approved by NRC. 2-1 The components for CGD are CPCS, PPS, ESF-CCS, QIAS-P, ITP, ESCM, CCG, and OM which are implemented on common PLC platform, and flat panel display for safety I&C system, as shown in Figure 4.1-1 of the Safety I&C System TeR. The critical characteristics of Common-Q have been already identified through preliminary phase and follow-up phase during CGD process.

The second choice will be[ ]which has been developed in accordance with 10 CFR 50 Appendix B and is not necessary for CGD.

The specific platform will be selected at COL stage. If it is necessary to provide additional information on the characteristics, we will develop such requirement from the above platform.

3. CPCS items relating to the KEPCO & KHNP SAFETY I&C SYSTEM TeR, APR1400-Z-J-EC-13001-P Rev.0:
   a. Determination of Failures relating to redundant measurement/data paths:
      i. Clarify what constitutes a RPST is failed when determining "less than four RSPT signals are failed" or "four or more RPST signals are failed," as referenced in "(2) Compliance to DI&C-ISG-04, Position 2" on page C-30. Is this failure count based solely on the RPST sensor inputs directly monitored by a CEAC Rack, or does it include RPST sensor data provided by an interchannel communication SDL?

Response

The Reed Switch Position Transmitter (RSPT) failures are defined as follows;

[ ]

Any of above failures is declared as the RSPT failures.
If there are RSPT failures more than four, CEAC will set CEAC failure flag by itself.
RSPT failure count includes RSPT sensor data provided by an inter-channel communication SDL.

ii. Clarify what constitutes a RPST 1 (or 2) is failed when determining "four or more RSPT1 signals are failed and four or more RSPT2 signals are failed," as referenced in "(2) Compliance to DI&C-ISG-04, Position 2" on page C-30. Is this failure count based solely on the RPST sensor inputs directly monitored by a CEAC Rack, or does it include RPST sensor data provided by an interchannel communication SDL?

<u>Response</u>

If there are RSPT failures more than four, CEAC will set CEAC failure flag by itself.
RSPT failure count includes RSPT sensor data provided by an inter-channel communication SDL.

b. Response to Failures relating to redundant measurement/data paths:

i. Clarify what safety analysis has been performed to demonstrate the equipment behavior in the presence of RPST failures is conservative (e.g., produces a conservative Penalty Factor under all degrees of failures RPST regardless of quadrant and until a channel issues a fail-safe trip action vote).

<u>Response</u>

The FMEA for CPCS sensor failure is described in DCD Section 7.2 (No 2-4).
The equipment behavior in the presence of RSPT failures is as follows:

- If a failure of redundant RSPTs is detected by AI or Processors, the sound RSPT signal is used in CEAC and CPC calculation to avoid a spurious trip.
- If the failure of RSPT is undetected by diagnostic, CPC use the more conservative value (bigger PF value) of redundant RSPTs to make trip to PPS.

These are requirements from CPCS design and will be verified through V&V processes.

c. Consideration of SW CCFS:

i. Clarify how the diversity analysis addresses common-cause failures due to programming within the CPCS that might cause all four channels to fail to perform a safety function (e.g., High Local Power Density, etc.).

<u>Response</u>

The diversity is not considered for CPC and CEAC software. The CPC and CEAC software are identical among all channels. Otherwise, the CPP software which is responsible for inter-channel communication among four channels is not identical.

As described in page C-1 of the D3 TeR, the D3 analysis assumes the total functional loss of safety PLC based systems in case of CCF. This analysis is considering that the common cause failures might cause all safety systems which are implemented on the same platform fail to perform a safety function.

The CCFs within CPCS software are considered the same as CCFs of PPS software. In the D3 TeR, DPS and manual switches are used to mitigate AOOs and accidents.

ii. BTP 7-19 provides acceptance criteria for diversity and defense-in-depth analysis that applies to anticipated operational occurrences (AOOs) in addition to postulated accidents. As described, all four channels of CPCS will contain nearly identical (if not identical) software designs although each channel independently monitors different RPST sensors and two channels monitor 23 RPSTs while the other two monitor 70 RPSTs. The CPCS creates both DNBR and LPD trips, which are credited in Chapter 15. The CCF Coping Analysis TeR states: "For the DCD Chapter 15.4 case, the uncontrolled withdrawal transient is terminated by either a variable overpower trip, high pressurizer pressure trip, a low DNBR trip or high local power density depending on the initial conditions and reactivity insertion rate." This addresses 15.4.2 "Uncontrolled Control Element Assembly Withdrawal at Power." However, the staff could not see where DNBR function was addressed for 15.1 (e.g., 15.1.1 "Decrease in Feedwater Temperature, 15.1.3 "Increase in Steam Flow," etc.). Furthermore, the staff could not similarly identify where the LPD function was addressed. The staff notes that Chapter 15 Table 15.0-7 (1 of 5) does not identify the CPCS or the DNBR or LPD for 15.1.1 and 15.1.3, despite the descriptions provided in those sections. The staff does not understand the reason for this apparent inconsistency.

Response

The “N/A” in Table 15.0-7 of Chapter 15 means the event is not considered as a limiting AOO in the 15.1 event category.
Event 15.1.4 is the most limiting AOO event for the 15.1 event category. The reactor trip and ESF functions are considered for that event only.

d. Evaluation per BTP 7-21:

i. The application does not provide information to support an evaluation using BTP 7-21, specifically an allocation of time delays to elements of the system and software architecture, including an estimated allocation of time delays to elements of the proposed architecture, that are based on the characteristics of the proposed computer hardware, software, and data communications systems.

Response

The response time requirements are provided in Table 7.2-5 of the DCD Tier 2. Total response time encompasses from sensor to input terminal of actuation device.

Followings are examples of SKN3&4 CPCS response time analysis results for information.

For simple CPCS signal path,[ ] of response time requirement is allocated. The time excludes sensor delay time, PPS delay time, and actuator delay time (CPCS times only).

Figure 1 shows the component based response time assignment for the above parameters except CEA related trips.
For the RSPT signal inputs which are provided by inter-channel SDL, the Figure 2 shows the component based response time assignment including communication delay.

[ ]TS

Figure 1 Response Time Analysis for CPC Simple Signal Path

Total response time of CPC is[.] Therefore, this analysis shows that the response time is not exceed the response time requirements ( ).

[ ]TS

Figure 2 Response Time Analysis for CPC Complex Signal Path

From Table 7.2-5 of DCD, CEAC Penalty Factor trip signal response time requirement must be no longer than[ ].
The response time requirements for subsystem are divided into[ ] for CPCS processing,[ ] for PPS discrete signal processing, and [ ] for Reactor Trip Switchgear System.

All control modules (CTRLM) in the CPCS are assumed to have[ ] percent of CPU loading. In this case, worst case CTRLM processing time is[ ] times of one CPU cycle time (CT).

Figure 2 shows one of the longest signal path for CEAC Penalty Factor calculation. CEAC CTRLM receives data from the alternate HSL communication path when preferred HSL path is unavailable.

In Figure 2, worst case response times of CTRLMs and HSLs are calculated as follows:

- CPP CTRLM 1 (Worst case CT in other CPCS channel) = [ ]
- CPP CTRLM 1 (Worst case CT in CEAC processor subrack) = [ ]

- CPP CTRLM 3 (Worst case CT in CEAC processor subrack) = [ ]
- CEAC CTRLM (Worst case CT in CEAC processor subrack) = [ ]
- CPC CTRLM (Worst case CT in CPC processor subrack) = [ ]
- High Speed Link (HSL) communication time delay =[ ]

The total response time of CPCS for CEAC Penalty Factors trip signal generation is 563 ms as shown in Figure 2.
This time result shows that the worst case response time is not exceed the response time requirement that allocated to CPCS [ ]

ii. The BTP 7-21 provides acceptance criteria including 1) "limiting response times be shown to be consistent with safety requirement," 2) "digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems," 3) "An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available," and 4) "The timing budget should include internal and external communication delays, with adequate margins."

Response

The limiting response times are provided in table 7.2-5 in DCD Tier-2.

The digital computer timing, an allocation of time delays to elements of the system and software architecture, and the timing budget are described in the answer of 3.d.i.

iii. Table 7.1-1 indicates BTP 7-21 applies to all of I&C Systems identified in the table. However, the CPCS (as well as other systems) are not listed in Table 7.1-1. Furthermore, Section 7.1.2.74 states "response time requirements are described in the Setpoint Methodology for Plant Protection System TeR." This TeR's Acronym list provides DRT (Derived Response Time), SRT (Sensor Response Time), SDT (Signal Delay Time), and TART (Total Analysis Response Time). Regardless, the Setpoint Methodology for Plant Protection System TeR does not provide response time requirements, because it does not define a time or its allocation of times among I&C components associated with the Safety I&C architecture. The TeR does not identify sensor SRTs, or functional processor—including A/D conversion—and communication processor SDTs that are consistent with the architecture and components described in the Safety I&C TeR. Instead the Setpoint Methodology for Plant Protection System TeR uses the response time acronyms to describe certain Trip Setpoint calculations in an high level algebraic equation form, which correlates somewhat to Table 15.0-2, which in turn correlates somewhat to Table 7.2-5. Regardless, although referenced in Tables 15.0-2 and 7.2-5, neither DNBR nor LPD are addressed in the Setpoint Methodology for Plant Protection System TeR Appendices, because DNBR and LPD are defined as fixed values in the TeR's Section 2.3. Therefore, the high level algebraic equation was not provided for DNBR and LPD.

Response

The CPCS will be included in Table 7.1-1.

Setpoint Methodology for PPS TeR identifies just calculation method about how the total analysis response time requirement is met on the system basis.

The separate TeR for response time will be provided later (by June 2014). This report describes how the sum of allocated response times of individual components meet the total response time requirement assumed in the safety analysis listed in Tables 7.2-5 and 7.3-7 of the DCD Tier 2.

The response time allocations for individual components such as sensor, input module, processor module, communication, output module and relay are assumed based on the timing analysis and the response time test measurements in the reference plant (Shin-Kori 3&4) because the platform specific information is not available.

Also, at COL stage, the response time analysis including the potential impact of data throughput and data error rates based on vendor information will be performed to verify if it is less than the allocated response time.

Allocation of times among I&C components associated with the Safety I&C architecture will be added in Setpoint Methodology for Plant Protection System TeR.

Allocation of times for CPCS is provided in the answer 3.d.i.

- Setpoint methodology for CPCS

The CPCS is designed to provide the low DNBR and LPD reactor trips to ensure that the specified acceptable fuel design limits on departure from nucleate boiling (DNB) and centerline fuel melt are not exceeded during AOOs. The CPC system initiates the reactor trips based on low DNBR and high LPD trip setpoints.
Overall uncertainties are used to determine limiting safety system settings for CPCS DNBR and LPD trips.

Followings are the high level algebraic equations for DNBR and LPD setpoint calculation.

[DNBR AND LPD TRIP SETPOINT CALCULATION]

TS

TS

•
•
•
•
•
•

TS

Figure 3 Application of BERRi

Figure 3 shows the place where each BEER is used.

Detailed methodology for CPCS overall uncertainty analysis is described

TS

iv. The CPCS is safety I&C that creates DNBR and LPD protective actions The staff notes that the CPCS response time requirements may be more complicated than others. The CPCS description along with Figure 4.3-1 indicate redundant paths for CEA position data are available from the RPST source analog inputs to individual function processors (CPPs, CEACs, and CPCs). The CPCS description also indicates either a primary or backup RPST signal may be used. Finally, the CPCS description explains that either a preferred and alternate SDL may be used to provide the CEA position data depending on other failures. Application information should include information to support an evaluation using BTP 7-21. For the CPCS, the application information should ensure that variable propagation and processing delays for CEA position data to safety function vote have been analyzed and tested to demonstrate BTP 7-21 has been adequately addressed by the CPCS design.

Response

Variable propagation and processing delays for CEA position data are incorporated in the CPCS design. The interfaces from CPCS to PPS are hardwired. The delay time of the bistable and voting logics in the PPS are described in the answer 4.i.

4. Evaluation per DI&C-ISG-04:

   i. The application does not provide sufficient information to support a complete evaluation using DI&C-ISG-04, specifically the potential impact of data throughput and data error rates on worst-case response time.

Response

The RPS and ESFAS are designed to meet the response time requirements listed in Table 7.2-5 and 7.3-7 of the DCD Tier 2 which are required by Chapter 15 safety analyses.

APR1400 has opted “platform-neutral” approach and platform specific analysis results are provided at ITAAC closing stage.   The results include analysis of timing budget for each module and the bandwidth for the communication to verify if the worst-case response time meets the response time requirements.

The response time testing in ITAAC item 17 of Table 2.5.1-5 and item 21 of Table 2.5.4-4 in the DCD Tier 1 shall verify that the RPS and ESFAS fulfills the response time criteria under maximum CPU loading. Also, the tests will be performed to ensure that the data throughput including the potential impact of data error rates is less than the communication bandwidth.

The below is a typical example of reference plant SKN3&4 showing how to present to meet the response time requirements.

For example, the response time requirement for High Pressurizer Pressure is 0.85 second (850 ms) as shown in Table 7.2-5.

System design requirements for PPS are as follows:

[
•
•
•
]TS

The total response time requirements (525 ms) are selected conservatively shorter than safety analysis requirement of High Pressurizer Pressure trip signal path (850 ms).

Detail response time analysis of PPS cabinet for the worst case conditions are as follows:

[•
•
•
•
•
•]TS

The total sum of the above response time is[ ], which is less than the response time requirement of the system design [.]

The response time of HSL communication was calculated considering the following factors:

[•
•
•]TS

[ ]TS

ii. Staff Positions 1.19 and 1.20 of DI&C-ISG-04 address the potential impact of data throughput and data error rates on worst-case response time. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate, which is supported by the error rate observed in design and qualification testing. As such, actual error rates should be observed through design and qualification testing to be less than the design basis communication error rates used in system response time calculations. However, the application does not demonstrate observed communication error rates are less than design basis communication error rates used in system response time calculations.

Response

The response time testing in ITAAC item 17 of Table 2.5.1-5 and item 21 of Table 2.5.4-4 in the DCD Tier 1 shall verify that the RPS and ESFAS fulfills the response time criteria.

At COL stage, the response time will be analyzed to verify if the worst-case response time assuming a data error rate meets the response time requirements. 4.ii-2 The qualification test will be performed to ensure that the actual data error rates is less than the communication error rates assumed in in the response time analysis.

iii. Appendix C of the Safety I&C TeR identifies the applicability of DI&C-ISG-04 and explains high level architectural aspects of the serial data links at a high level. However, Appendix C of the Safety I&C TeR does not provide information to address the characterization of serial data link protocol performance for design basis communication error rates, failure detection, and demonstration of continued adequate performance with respect to safety function response times.

Response

At COL stage, the information to address the characterization of serial data link protocol performance for design basis communication error rates, failure detection, and demonstration of continued adequate performance with respect to safety function response times will be provided.

The below is an example information of serial data link of SKN3&4.

TS

•
•
•

•
•
•

•

5. For all events indicative of ATWS described in the application, will the APR-1400 I&C system initiate a turbine trip, start aux feedwater, and initiate a diverse reactor scram concurrently? Chapter 15 of the APR-1400 FSAR seems to indicate that these actions will occur concurrently, however Chapter 7 seems to indicate that for some events, the I&C system will initiate a turbine trip and others it will only initiate aux feedwater. Address this inconsistency.

Response

As described in Section 15.8.3 of the APR 1400 DCD, the diverse protection system (DPS) provides a diverse backup to the PPS. The functions of DPS are composed of diverse reactor trip, auxiliary feedwater actuation, actuation of safety injection and turbine trip; and all of these DPS functions will not be occurred concurrently.

The diverse reactor trip signal is generated when it reaches the preset value on high pressurizer pressure or high containment pressure. Turbine trip by the DPS is occurred after the diverse reactor trip with three seconds time delay. The actuation of auxiliary feedwater system by the DPS is initiated on low steam generator level and is not related to reactor trip and safety injection. And the actuation of safety injection system by the DPS is initiated on low pressurizer pressure and is not related to reactor trip and auxiliary feedwater actuation.

As described in Section 4.1.3.1 of the Safety I&C System TeR, the DPS setpoints are specified so that the PPS automatic trip/actuation signals occur before the generation of DPS signal.

Section 15.8.3 describes that the DPS provides a diverse backup to the PPS.
The following description in Section 15.8.3 will be clarified in the next revision of the DCD:

[Current description]
The DPS initiates a reactor trip signal on high pressurizer pressure to decrease the possibility of an ATWS and provides an auxiliary feedwater actuation signal (backup to the ESF-CCS of the PPS) to provide reasonable assurance that an ATWS event is mitigated if it occurs.

[Description to be revised]
The DPS initiates a reactor trip signal on high pressurizer pressure to decrease the possibility of an ATWS. The DPS also provides an auxiliary feedwater actuation signal on low steam generator level (as a backup to the ESF-CCS of the PPS) to provide reasonable assurance that an ATWS event is mitigated if it occurs.