UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

September 25, 2017

Mr. Victor M. McCree
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: INTERIM LETTER: CHAPTERS 7 AND 18 OF THE NRC STAFF'S SAFETY EVALUATION REPORT WITH OPEN ITEMS RELATED TO THE CERTIFICATION OF THE APR1400 DESIGN

Dear Mr. McCree:

During the 646th meeting of the Advisory Committee on Reactor Safeguards, September 7-8, 2017, we met with representatives of the Korea Electric Power Corporation and Korea Hydro & Nuclear Power Company, Ltd. (KHNP), and the NRC staff to review the following chapters of the safety evaluation report (SER) with open items associated with the APR1400 design certification application:

- Chapter 7, "Instrumentation and Controls"
- Chapter 18, "Human Factors Engineering"

Our APR1400 Subcommittee reviewed these chapters during meetings on June 20-21, 2017. We also had the benefit of the referenced documents.

CONCLUSION AND RECOMMENDATIONS

1. Our review of Chapter 18 did not identify any issues with potential safety implications that merit attention at this stage of the review.

2. Regarding Chapter 7, the staff should ensure that:

    - A detailed explanation of operation of the Common Q™ PM646 watchdog timer functions is provided to clarify how division to division voting independence is not compromised.

    - A detailed description of the one-way, hardware-based data diode (not controlled or configured by software) is provided to demonstrate complete isolation from external communications.

BACKGROUND

KHNP submitted a design certification application for the APR1400 on December 23, 2014. Our review is being conducted on a chapter-by-chapter basis to identify technical issues that may merit further consideration by the staff. This process will aid in resolution of concerns and facilitate timely completion of the design certification review. The staff's SER and our review of these chapters addressed Design Control Document (DCD), Revision 0, and supplemental material, including KHNP responses to staff requests for additional information.

DISCUSSION

During the Subcommittee presentations of these chapters, the staff identified a significant number of open items. Many of the open items have been closed or a pathway to resolution has been identified. We have not identified any issues with Chapter 18 that merit attention at this time. However, additional clarification is needed with respect to two items in Chapter 7.

The DCD, Tier 2, Chapter 7, Revision 0, and associated technical report, APR1400-Z-J-NR-14001-P, "Safety I&C System," Revision 0, describe how the digital instrumentation and control (DI&C) system meets the fundamental design principles of independence, redundancy, predictability and repeatability, diversity and defense in depth, and control of access. They also describe the testing and diagnostic concepts used in the system design. The staff SER with open items concludes that the APR1400 DI&C safety system should meet the fundamental principles subject to satisfactory resolution of currently identified open and confirmatory items.

Control of access was evaluated only from the standpoint of physical and administrative access to the DI&C safety system. The SER states that IEEE Std. 603-1991, Section 5.9, requires that the safety system design permit the administrative control of access to safety system equipment. NUREG-0800, Section 7.9, states that remote access to safety systems should not be implemented. Presentations during the June 20, 2017, APR1400 Subcommittee meeting identified virtual local area network (VLAN) switches for communication external to the plant. It was stated that the VLAN switches included a firewall that prevents inbound communication using a hardware-based, unidirectional interface. However, there was no mention or description of the VLAN switches and the hardware-based, unidirectional outbound-only firewall in DCD, Chapter 7, or the "Safety I&C System" technical report. The staff should ensure that a detailed description of the one-way, hardware-based data diode (not controlled or configured by software) is provided to demonstrate complete isolation from external communications.

The APR1400 uses the Common Q™ software-based micro-processor platform for plant parameter detection and trip determination and the same platform for 2 out of 4 coincidence voting independently in each of the four reactor trip and engineered safeguards actuation divisions. This platform has been used in other new-plant designs for reactor trip and engineered safeguards actuation. We previously reviewed these applications.

The basis for acceptance of the use of the Common Q™ platform for the 2 out of 4 coincidence voting in the earlier projects was the inclusion of an analog, hardware-based watchdog timer. The purpose of the watchdog timer is to monitor the microprocessor. Should the microprocessor lock up, the watchdog timer would produce a reactor trip signal for that division and an alarm for the engineered safeguards actuation for that division. This basis was also proposed as the acceptance criterion for APR1400.

The attachment to this letter summarizes our understanding of the current status of an issue related to the use of watchdog timers in the Common Q™ platform. For application of this platform in the APR1400 design, the staff should ensure that sufficient information is provided to answer the following questions:

1. The most recent revision to the topical report states that the window watchdog timers are hardware-based. The description in the topical report seems to have them intertwined with operating system software, in particular the Task Scheduler, SYSDia, and Configuration Task. How are the window watchdog timers diverse and why is the nature of the diversity equivalent to a strictly hardware-based, software-independent design?

2. If the hardware-based watchdog stall timer external to the central processing unit (CPU) could be disabled by the base operating system software design, why are the window watchdog timers not susceptible to the same problem?

3. What is the nature of the Common Q™ PM646 module trigger signal to the window watchdog timers? Is it a bistable output or is it a signal developed by the system software?

We look forward to further interactions with the staff to answer our questions. Additional comments by ACRS Member Jose March-Leuba are presented below.

Sincerely,

/RA/

Dennis C. Bley
Chairman

Attachment
Common Q™ Watchdog Timer Background

The Common Q™ platform was initially described in topical report CENPD-396-P, "Common Qualified Platform," Revision 0; CENPD-396-P, Revision 1 was issued in May 2000. The NRC issued an SER for CENPD-396-P, Revision 1, dated August 11, 2000 and a subsequent SER dated February 24, 2003. The SER generic open items which were closed in the February 24, 2003 SER culminated, in part, in the issuance of WCAP-16097-P-A, "Common Qualified Platform," Revision 0 (also identified as CENPD-396-P, Revision 2), in May 2003.

WCAP-16097-P-A, Section 2.1, "Common Q System," stated that an external watchdog timer module has a timing function to detect the lack of activity of the processing system. Depending on the application, the watchdog timer can be used to annunciate a failure, actuate a channel trip, or set output states to predefined conditions. Section 4.1.5, "Watchdog Timer Module," stated that information on the design or dedication of the hardware watchdog timer had not yet been submitted.

Item 3 in Section 3.2.2.1, "Changes to the Common Q TR," of the SER, dated February 24, 2003, for CENPD-396-P, Revision 1, stated that all references to the external watchdog timer in the topical report and its appendices have been changed to reflect the use of the main processor module PM646A built-in hardware watchdog timer function in lieu of an external watchdog timer. The built-in hardware watchdog timer function consists of a relay driven by analog circuitry and can be used to annunciate a failure, actuate a channel trip, or set output states to predefined conditions. In Section 3.1 of the February 24, 2003 SER, the staff concluded that Westinghouse has acceptably qualified the built-in hardware watchdog timer function in the PM646A processor module for use in safety systems in nuclear power plants. Thus, substitution of the built-in watchdog timer function meets the applicable regulatory requirements. Generic open item 7.3, related to the watchdog timer, opened by the staff in the August 11, 2000 SER was closed in the February 24, 2003 SER.

This was the approach presented for the earlier design reviews and was what we assumed was intended for the APR1400 Common Q™ application.

The Common Q processor module was designed with four separate timers, sometimes known as watchdog timers:

1. Software stall timer (also known as the software watchdog timer or CPU watchdog timer): internal to the microprocessor
2. Hardware stall timer (also known as the external hardware watchdog timer or external CPU watchdog timer): external to the microprocessor
3. Window watchdog timer: located on the processing section of the processor module, external to the microprocessor
4. Window watchdog timer: located on the communication section of the processor module, external to the microprocessor

After our June Subcommittee meeting, Westinghouse issued Nuclear Safety Advisory Letter NSAL-17-2. Westinghouse disclosed that the software stall timer (1) was never activated in the AC160 base software, which then disabled the hardware stall timer (2). The window watchdog timers (3 and 4) remained fully functional. By design, the stall timers provide diagnostic functions

following a severe software fault and are not required for the system to perform its safety-related functions. The window watchdog timers are a diverse and non-software based watchdog that will actuate for the same and other severe software faults as the stall timers (1 and 2) and will activate the single watchdog timer relay to perform the safety-related functions. It is these window watch dog timers that were credited for closing generic open item 7.3 in the February 24, 2003 SER for CENPD-396-P, Revision 1.

Additional Comments by ACRS Member Jose March-Leuba

Watchdog Timers

The APR1400 plant protection system is based in part on the Common Q™ programmable logic controller platform, which was reviewed and approved by the staff in 2013. The Common Q™ platform has four diverse watchdog timers. After the staff review of Chapter 7 was completed, the Common Q™ vendor discovered that one of the watchdog timers was not activated in their initial hardware implementation. Based on a preliminary review of the data in July 2017, the vendor concluded that the remaining watchdog timers would satisfy the licensing bases to provide the required diversity function. The staff has not yet reviewed this event and has not reached a position on the Common Q™ generic applicability without the failed watchdog timer.

KHNP has stated that the APR1400 is based on the Common Q™ platform as approved by the staff's 2013 SER. Thus, the APR1400 Common Q™ hardware implementation will include all the features of the approved licensing topical report, including all watchdog timers. Furthermore, KHNP has stated that, should the licensing bases for the Common Q™ platform change before APR1400 implementation, they must follow the new licensing bases or justify an exception and request staff approval. This approach is acceptable for APR1400 because either: (1) the failed watchdog timer will be activated in APR1400, or (2) a future staff review will conclude that the fourth watchdog timer is not needed to satisfy the diversity requirement. In addition, it is acceptable for the APR1400 certification to follow the standard process, where an applicant takes advantage of already approved methodology (in this case the Common Q™ SER). Should additional information invalidate the licensing bases of the approved methodology, the APR1400 must follow the approved methodology as revised at the time of construction.

Firewall

The APR1400 design includes an external data communication path to the plant emergency operation facility and the NRC emergency response data system. The path ensures unidirectional communications using a hardware-based firewall, which includes fiber optic links. As with most I&C systems, the APR1400 DCD does not specify the particular hardware that will be used for all future licensing requests; instead, it specifies its requirements. In this case, the DCD specifies that the external data communication must be implemented using: (1) fiber optic links, which minimize the potential for electromagnetic interference that could occur if copper cable was used, and (2) one-directional hardware devices. It is acceptable for a DCD not to specify the particular hardware implementation and only specify the functional requirements, which is the standard process for most I&C systems.

REFERENCES

1. U.S. Nuclear Regulatory Commission, “Advanced Power Reactor 1400 Design Certification Application – Safety Evaluation with Open Items for Chapter 7, ‘Instruments & Controls’,” May 23, 2017 (ML17139C682).

2. U.S. Nuclear Regulatory Commission, “Advanced Power Reactor 1400 Design Certification Application – Safety Evaluation with Open Items for Chapter 18, ‘Human Factors Engineering’,” May 17, 2017 (ML17103A024).

3. Korea Electric Power Corporation and Korea Hydro & Nuclear Power Company, Ltd., “Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd Application for Design Certification of the APR1400 Standard Design,” December 23, 2014 (ML15006A098).

4. Korea Electric Power Corporation and Korea Hydro & Nuclear Power Company, Ltd., “Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd, Technical Report, APR1400-Z-J-NR-14001-P, ‘Safety I&C System’,” Revision 0, November 2014, (ML15009A324).

5. IEEE 603-1991, “IEEE Standard - Criteria for Safety Systems for Nuclear Power Generating Stations,” June 27, 1991.

6. U.S. Nuclear Regulatory Commission, NUREG-0800, Standard Review Plan Chapter 7.9, “Data Communication Systems,” Revision 6, August 2016 (ML16020A097).

7. CE Nuclear Power LLC, CENPD-396-P, “Common Qualified Platform,” Revision 1, May 2000 (ML003721641).

8. U.S. Nuclear Regulatory Commission, Safety Evaluation, “Safety Evaluation by the Office of Nuclear Reactor Regulation CE Nuclear Power Topical Report CENPD-396-P ‘Common Qualified Platform’ Project No. 692,” August 11, 2000 (ML003740165).

9. U.S. Nuclear Regulatory Commission, “Acceptance of the Changes to Topical Report CENPD-396-P, Revision 1, ‘Common Qualified Platform,’ and Closeout of Category 2 Open Items,” February 24, 2003 (ML030550776).

10. Westinghouse Electric Company, WCAP-16097-P-A, “Common Qualified Platform,” Revision 0, May 2003 (ML031830959).

11. Westinghouse Electric Company, Nuclear Safety Advisory Letter NSAL-17-2, “AC160 Processor Module Stall Timers Not Activated as Described in Licensing Basis,” July 5, 2017 (ML17213A208).

12. Westinghouse Electric Company, WCAP-16097-P-A, “Common Qualified Platform,” Revision 3, February 2013, (ML13081A065).

13. U.S. Nuclear Regulatory Commission, “Final Safety Evaluations for Topical Report WCAP - 16097, Revision 3, ‘Common Qualified Platform Topical Report,’ (TAC No. ME5157) and WCAP-16096-P/NP, ‘Software Program Manual for Common Q Systems’ (TAC No. ME5159),” February 7, 2013 (ML13022A124).

13. U.S. Nuclear Regulatory Commission, “Final Safety Evaluations for Topical Report WCAP - 16097, Revision 3, ‘Common Qualified Platform Topical Report,’ (TAC No. ME5157) and WCAP-16096-P/NP, ‘Software Program Manual for Common Q Systems’ (TAC No. ME5159),” February 7, 2013 (ML13022A124).

Accession No: ML17265A792 **Publicly Available Y** **Sensitive N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	**ACRS/TSB**	**SUNSI Review**	**ACRS/TSB**	**ACRS**	**ACRS**
NAME	CBrown	CBrown	MBanks	AVeil	DBley (AV for)
DATE	9/25/17	9/25/17	9/25/17	9/25/17	9/25/17

OFFICIAL RECORD COPY