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

March 15, 2012

Mr. R.W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: CHAPTERS 6, 7, 11, 13, 15, 16, AND 18 OF THE SAFETY EVALUATION REPORT WITH OPEN ITEMS ASSOCIATED WITH THE U.S. EVOLUTIONARY POWER REACTOR DESIGN CERTIFICATION APPLICATION

Dear Mr. Borchardt:

During the 592nd meeting of the Advisory Committee on Reactor Safeguards (ACRS), March 8-10, 2012, we met with representatives of the NRC staff and AREVA NP, Inc., (AREVA or the applicant) to review the following chapters of the Safety Evaluation Report (SER) with Open Items associated with the U.S. Evolutionary Power Reactor U.S. (EPR) design certification application:

- Chapter 6, “Engineered Safety Features,” except for Section 6.2.1.2, “Subcompartment Analysis,” and Section 6.2.2, “Containment Heat Removal”;
- Chapter 7, “Instrumentation and Controls”;
- Chapter 11, “Radioactive Waste Management”;
- Chapter 13, “Conduct of Operations”;
- Chapter 15, “Transient and Accident Analysis,” except for Section 15.6.5, “Loss of Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary”;
- Chapter 16, “Technical Specifications”; and
- Chapter 18, “Human Factors Engineering.”

Our EPR Subcommittee reviewed these chapters during meetings on April 6, 2010, November 10, 2010, February 7-8, 2011, April 5, 2011, August 18, 2011, and November 14, 2011. We also had the benefit of the documents referenced.

CONCLUSIONS

1. The staff has identified appropriate open items in its review of the chapters of the U.S. EPR design certification application identified above and can move to resolution of these open items.

2. We have identified four additional issues in connection with these chapters that staff should consider as they resolve the open items:

    - Inadequate characterization of the "watchdog" timer design in the instrumentation and control system and the independence of these devices.

    - The importance of human activities should not be weighted by the frequency of the plant operating mode.

    - Allowance for operation with only three reactor coolant pumps should be reviewed considering reverse flow in the idle loop, changes in reactor coolant system flow, and lack of symmetry in the flow across the plane of the lower core distribution plate.

    - The algorithm for evaluation of the departure from nucleate boiling ratio (DNBR) should account for the possibility of non-uniform flow in channels due to such things as lower plenum flow anomaly or three-loop operation.

DISCUSSION

The NRC staff has adopted a multiple phase approach to the review of the U.S. EPR design certification application. Phase 3 of this strategy involves our review of the draft Safety Evaluation Report with Open Items. This review affords us an opportunity to identify issues meriting staff attention prior to finalization of the Safety Evaluation Report. The review is done on a chapter-by-chapter basis. Consequently, our review of the application and safety evaluation should not be construed as final. Indeed, final review by the ACRS is done in the fifth phase of the staff strategy when we can examine the Safety Evaluation Report as an integrated whole.

We have reviewed the seven chapters of the staff's Safety Evaluation Report listed in the opening of this letter. We conclude that staff has adequately identified open items that must be resolved prior to finalizing the Safety Evaluation Report. We agree that pathways are available for staff and the applicant to resolve these open items. The materials we have reviewed in these chapters can be moved to the fourth phase of the staff review strategy.

We have identified four issues that should be considered by the staff as they resolve open items in these chapters:

- Digital safety systems in the U.S. EPR use software-based processing for computations and voting units in each division. Common-cause failure can lead to a "lockup" of these systems. To avoid safety hazard from such "lockups," the applicant has incorporated so-called "watchdog" timers. The documentation provided to us is inadequate to assure that the designs for these watchdog timers are immune to software common-cause failure. It is not evident how the timers will accomplish their trip functions. We have not been convinced that the Target System Hardware Interface that accesses the watchdog timers will not compromise their independence.

- The applicant has identified risk-important human actions to be considered in the human factors engineering design. They have, however, weighted the assessment of the importance of human actions by the frequencies of the plant operating modes. Human actions that can endanger the safety of the plant need to be identified regardless of the duration of the pertinent plant operating mode.

- The U.S. EPR design allows for up to two hours of operation with only three reactor coolant pumps. Our experience indicates that staff should review this provision by carefully considering the effects of reverse flow in the idle coolant loop, reductions in the reactor coolant system flow, and the lack of symmetry in flow across the plane of the lower core distribution plate.

- The algorithm used to determine the minimum DNBR utilizes measured values for the core inlet temperature, total core flow, reactor pressure, and local neutron flux. The DNBR algorithm does not appear to account for the possibility of non-uniform flow within the core channels which might be caused by a lower plenum flow anomaly or three-loop operation.

The NRC staff has advised us that the applicant has submitted a topical report describing scaled experiments that support the assumption of uniform flow. We would appreciate the opportunity to review this topical report.

The Distributed Control System functional architecture includes networks separated from the Plant Business Networks by firewall units. There are no design details explaining how these firewalls will be configured to be a "one-way" information highway that cannot be corrupted. Malicious "hacking" of the single entry point firewalls could corrupt data transmitted to the main

control room, the remote shutdown station, and the technical support center. Though cyber security is not part of our current review of the U.S. EPR Safety Evaluation Report, design details that assure the information pathways to the Plant Business Networks cannot be altered by external commands or other means should be specified in the design control document.

Dr. J. Rempe did not participate in our discussions of this matter.

Sincerely,

/RA/

J. Sam Armijo
Chairman

REFERENCES

1. AREVA NP Letter, "Application for Standard Design Certification of the U.S. EPR (Project No. 733)," dated December 11, 2007 (ML073520305)

2. AREVA NP Letter, "Submittal of Revision 1 of the U.S. EPR Final Safety Analysis Report for Design Certification," dated May 29, 2009 (ML091670376)

3. AREVA NP Letter, "Submittal of Revision 2 of the U.S. EPR Final Safety Analysis Report for Design Certification," dated August 31, 2010 (ML102560479)

4. AREVA NP Letter, "Submittal of Revision 3 of the U.S. EPR Final Safety Analysis Report for Design Certification," dated August 10, 2011 (ML11230A572)

5. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Portions of Chapter 6, "Engineered Safety Features," dated March 24, 2011 (ML102850350)

6. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 7, "Instrumentation and Controls," dated October 17, 2011 (ML112580362)

7. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 11, "Radioactive Waste Management," dated March 5, 2010 (ML100251442)

8. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 13, "Conduct of Operations," dated July 7, 2010 (ML101040584)

9. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Portions of Chapter 15, "Transient and Accident Analyses," dated August 10, 2010 (ML101440207)

10. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 16, “Technical Specifications,” dated March 10, 2010 (ML093350144)

11. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 18, “Human Factors Engineering,” dated June 28, 2011 (ML1110840078)

10. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 16, “Technical Specifications,” dated March 10, 2010 (ML093350144)

11. NRC Memorandum, transmitting U.S. EPR Design Certification Application – Safety Evaluation with Open Items for Chapter 18, “Human Factors Engineering,” dated June 28, 2011 (ML1110840078)

Accession No: **ML12072A206** **Publicly Available** **Y** **Sensitive** **N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	KWeaver	KWeaver	CSantos	EMHackett	EMH for JSA
DATE	03/15/12	03/15/12	03/15/12	03/15/12	03/15/12

OFFICIAL RECORD COPY

Letter to Mr. R.W. Borchardt, EDO, from J. San Armijo, ACRS Chairman, dated March 15, 2012

SUBJECT: CHAPTERS 6, 7, 11, 13, 15, 16, AND 18 OF THE SAFETY EVALUATION REPORT WITH OPEN ITEMS ASSOCIATED WITH THE U.S. EVOLUTIONARY POWER REACTOR DESIGN CERTIFICATION APPLICATION

ML#12072A206

Distribution:
ACRS Staff
ACRS Members
L. Mike
B. Champ
A. Lewis
C. Jaegers
M. Orr
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRRPMAAdamsResource
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter