KEY MESSAGES ON DIGITAL INSTRUMENTATION AND CONTROL DESIGN

On the basis of the information submitted by AREVA NP (AREVA) for the U.S. EPR Instrumentation and Controls (I&C) systems design, the U.S. Nuclear Regulatory Commission (NRC) staff has determined that aspects of the design: (1) Do not meet regulatory requirements for functional independence; and (2) do not conform to regulatory guidance regarding communications, nor demonstrate acceptable alternatives to NRC-approved guidance.

A root cause of these issues is the complexity of the design itself. This complexity contributes to the design's inability to meet NRC requirements and guidance, and makes it unlikely that the design will be demonstrated or found acceptable in the timeframe desired by AREVA or the combined license applicants referencing this design.

I. With respect to regulatory requirements and guidance:

a) Aspects of the U.S. EPR I&C system design do not comply with NRC requirements. Specifically, the U.S. EPR I&C systems design does not meet the fundamental principle of independence as required by Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991 and the applicable regulations [i.e., Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 Section 55a(h) and 10 CFR Part 50, Appendix A (General Design Criteria (GDC) 21 and GDC 24)].

1. Several of the safety functions within the U.S. EPR design require information from outside their own division to accomplish the safety function.

   i. Sharing of processed in-core power sensor measurements among redundant safety divisions to accomplish Departure from Nucleate Boiling Ratio (DNBR) and Linear Power Density Reactor Trip functions.
   ii. Using the average of Protection System divisional core thermal power calculated output for the Safety Automation System to achieve Main Steam Relief Control Valve control for ESF actuation.

2. Protection of the Safety Automation System and Protection System from adverse influence from the non-safety-related Human Machine Interface (HMI) of Process Information and Control System (PICS) is provided with operator action from the safety-related HMI, Safety Information and Control System (SICS).

b) The U.S. EPR I&C system design does not conform to NRC regulatory guidance on communications independence nor the U.S. EPR design demonstrated acceptable alternatives to the NRC-approved guidance described in Interim Staff Guidance DI&C-SG-04, Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc), in those areas where the AREVA design does not conform to the identified acceptance criteria related to communications independence. Examples include:

1. Insufficient justification for why safety divisions need to receive any communication from outside their own safety division. These bi-directional data communication flows do not enhance or support a safety function.

2. No justification on why data exchange between redundant safety divisions or between safety and non-safety equipment is processed in a manner that does not adversely affect the safety function.

3. Insufficient justification for continuous connection between non-safety- related Service Unit and Safety Systems.

II. With respect to the complexity of the design contributing to both the inadequacies noted previously, and the likelihood of the design being demonstrated or found acceptable without modification:

a) AREVA has not demonstrated a clear understanding of how their design meets NRC regulations.

1. AREVA has not provided a complete list of interfaces and interconnections between redundant safety divisions and between safety systems and non-safety equipment. The NRC staff was able to identify more interfaces than those listed by AREVA in response to Request for Additional Information (RAI) 286.

2. AREVA has not provided adequate diagrams that clearly depict interconnections and data communications flow between systems.

3. AREVA has not recognized where the design does not meet NRC regulations, such as the case of the in-core power measurements, and relied on NRC staff to raise the issue.

b) The complexity of the design is not necessary to provide the required safety functions, and the complexity will require substantially more information to be submitted by AREVA and reviewed by the NRC staff.

1. Extensive interconnections exist between redundant safety divisions and between safety systems and non-safety equipment.

2. Most of these interconnections do not directly support or enhance the performance of safety functions, and create unnecessary complexity that outweighs any benefits from using bi-directional communication. The increased complexity can generate additional faults and failure modes in the design.

The NRC staff would need detailed design information, potentially including associated software, to be submitted on the docket in order to determine the acceptability of these interconnections. Such a review would require extensive resources and time to be

completed, both during initial certification and throughout the life of licenses issued for such a design.

The NRC staff concludes that the current U.S. EPR I&C Systems data communications design and system architecture do not meet NRC regulations. AREVA should incorporate a simpler data communication design that can be demonstrated to provide sufficient independence between redundant safety divisions, and between safety and non-safety equipment, to ensure safety function reliability.