



UK EPR GDA Project
A joint project of AREVA and EDF
QUBE
Whitfield Street
London
W1T 4EZ

**Joint Programme Office
Nuclear Reactor Generic Design
Assessment**

4NG Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS

Date 12 November 2010

Your ref: EPR70085R

Email: new.reactor.build@hse.gsi.gov.uk

Unique No: EPR70266N

TRIM ref: 2010/559769

Closure of Regulatory Issue RI-UKEPR-02

I write to inform you that we have now closed Regulatory Issue RI-UKEPR-02. The reason for this is that while there are some outstanding actions to complete, we are satisfied that you have addressed the majority of the key actions associated with the Regulatory Issue, and those that remain now equate to the status of a Regulatory Observation within the GDA process. We have raised RO82 to record formally this position.

I have attached, in an annex to this letter, a high level description of the rationale for our judgment.

We recognize that EDF and AREVA have put in a considerable amount of high quality work to get to this position. However I must remind you that RO82 is still very challenging and will require a high level of your attention and resource to successfully meet the UK EPR Programme.

We will be placing this letter on HSE's website alongside the associated RI.

Yours sincerely

Nuclear Directorate

Annex

Summary

In April 2009 HSE's Nuclear Directorate (ND) placed a Regulatory Issue (RI) on EDF and AREVA on the topic of the EPR Control and Instrumentation (C&I) System. The EPR is a reactor design submitted by EDF and AREVA (the Requesting Party (RP)) to the regulators for Generic Design Assessment (GDA). The outcome of the GDA for ND is a decision whether to grant a Design Acceptance Confirmation (DAC). An RI is an assessment finding of sufficient concern that if left unresolved would likely result in the decision to not grant the DAC.

This annex provides the rationale for closing the RI and for the remaining open RI actions being recorded now as Regulatory Observation (RO) actions. An RO, while still a finding requiring resolution, is at a lower level of importance than an RI and does not necessarily threaten the granting of a DAC.

UK EPR RI02

In April 2009, HSE's ND placed an RI on EDF and AREVA about its design of the EPR C&I.

The RI was based on four major concerns:

1. The complexity of interconnectivity between the very important Class 1 Safety Systems and lower Safety Class control systems. Of particular concern was that the lower Classes 2 and 3 Safety Systems could have write access to the highest Class 1 Safety System (the main Reactor Protection System). This also challenged our important safety assessment principle that Safety Systems should be completely independent of control systems.
2. There was a lack of Class 1 equipment including hard-wired and simple technology as a diverse backup to the highly computerised and sophisticated screen based displays and controls in the Main Control Room and Remote Shutdown Station.
3. The Class of many of the important control systems was Class 3 whereas our interpretation of the International Standards (IEC 61226:2009) was that such systems should be engineered to Class 2 standards.
4. The probabilistic claims being made on the two computer-based Safety System platforms meant that the common failure of both was equivalent to being 'incredible' so that the event could effectively be discounted.

The above constituted the main elements of the RI.

The response from EDF and AREVA

EDF and AREVA have addressed satisfactorily ND's concerns by proposing design changes to the C&I for the UK EPR. Taking each concern above In turn, the accepted response from EDF and AREVA has been as follows.

1. All networked communications will be one-way, from the Class 1 systems to lower Class 2 and 3 systems. The implementation will be through the isolation provided by one-way diodes. The permissive signals that were to be implemented through the lower Class systems will now be implemented using Class 1 Safety Information and Control System (SICS) equipment including a Qualified Display System.
2. There will be a Class 1 SICS operational in the Main Control Room and a similar panel in the Remote Shutdown Station. The SICS will include simple hard-wired technology and will be fully operational for alarms and displays at all times. Actuation signals from the SICS will be switched on if the Class 3 Plant Information and Control System fails.
3. Class 2 systems, rather than Class 3, will now provide the important station control systems. This will be achieved by reallocating functions to fully comply with IEC 61226:2009 and upgrading the Reactor Control and Surveillance Limitation system to Class 2.
4. Probabilistic claims on each of the main C&I platforms will have lower limits than in the original design for the UK. The shortfall in overall reliability of the safety systems will be made up by the introduction of a Non-Computer-Based Safety System (NCSS). The functions of the NCSS have been designed although details on the platform selection are still being evaluated by EDF and AREVA. However, they have given a commitment that the platform technology will be diverse to all hardware and software on the main Safety Systems.

The above changes represent a major step forward in addressing satisfactorily ND's concerns, and are the reason that we are now closing the RI. The remaining RI actions will be transferred to RO actions. ND is confident that in the next 6-18 months the submission, by EDF and AREVA, of detailed design information should be sufficient to allow closure of those RO actions, and that, in the interim, their extant status should not threaten the meaningful GDA Step 4 conclusion in June 2011.

November 2010