UK EPR GDA Project
A joint project of AREVA and EDF
1 Bedford Street
London
WC2E 9HG

Joint Programme Office
Nuclear Reactor Generic Design Assessment

4NG Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS

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

Date 16 April 2009

Your ref:

Unique No: EPR70085R

TRIM ref: 2009/152909

UK EPR Control and Instrumentation (C&I) Architecture
Regulatory Issue RI-UKEPR-002

I am writing to confirm our recent discussions where we have advised you that the issue of the adequacy of the UK EPR C&I architecture would be raised as a Regulatory Issue (RI).

Our C&I assessment work completed to date has identified the adequacy of the UK EPR C&I architecture as a matter of sufficient importance to raise this as a RI at this stage that may, if not resolved, prevent the successful outcome of GDA. Therefore, I have raised RI-UKEPR-2 to cover this topic. We have discussed our intention to issue this RI and outlined our concerns at our meeting in Erlangen on 13 and 14 January 2009 and more recently at the 13 March 2009 Level 4 teleconference. Our detailed concerns can be found below and in the Annex to this letter. You should also note that HSE ND has engaged a Technical Support Contractor to assist with its assessment of the UK EPR and as a result, additional matters relating to the C&I architecture (i.e. to those recorded in this letter) may emerge. Please note that the technical areas of concern given below and in the draft Regulatory Issue Actions (RIAs) attached were derived from our review of your proposed C&I architecture based on our Step 2 and Step 3 assessments against HSE's Safety Assessment Principles for Nuclear Facilities (SAPs), 2006 Edition, Revision 1. An important aspect of our SAPs is the strong emphasis on probabilistic safety analysis of complex systems in addition to the more traditional deterministic techniques. It is in the area of probabilistic analysis that some of the most significant challenges for the EPR C&I system arise particularly on matters of independence, diversity and the use of Class 2 and 3 systems with probabilistic claims in your Baseline Level 1 PSA more appropriate for Class 1 systems.

It is our regulatory judgement that the C&I architecture appears overly complex. Our judgement is based on a number of concerns; firstly, the reliance on two computer-based systems (originally developed by the same Company) and a high degree of connectivity between these two systems. Secondly, independence between the safety (Class 1) and the larger number of safety related systems (Class 2/3) appear to be significantly compromised due to the high level of interconnectivity between systems of different safety classification. Thirdly, we have serious reservations about your proposal which allows lower safety class systems to have write access (permissives etc.) to higher safety class systems (i.e. the usual UK practice of only allowing one way online communication from a safety system to systems of a lower safety class is not applied in the UK EPR design) (see Annex RI-UKEPR-2.A2). Other concerns include the absence of a safety class 1 display system (which is included in the Olkiluoto 3 (OL3) and US EPR designs) (see Annex RI-UKEPR-2.A3), no Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station (see Annex RI-UKEPR-2.A3) and EPR function categories/equipment class assignments do not appear to align with UK expectations as defined in BS IEC 61226 (see Annex RI-UKEPR-2.A4).

In addition EDF/Areva has now submitted its C&I PSA sensitivity study. HSE ND believes the baseline values used for C&I systems (i.e. 10^{-5} pfd for the Teleperm XS Protection System (PS) and 10^{-4} pfd for the Siemens SPPA -T2000 platform which provides back up reactor protection) will prove very difficult if not impossible to substantiate. The claim on the PS system is beyond the normal limit for reliability claims (i.e. 10^{-4} pfd) as stated in nuclear sector standards and guidance (Ref. 1, 2, 3, 4, 5, 6 and 7) including that of ASN's safety advisory group (Ref. 5). The claim for the Siemens SPPA - T2000, a Class 2/3 platform, is at the 10^{-4} pfd limit for Class 1 systems. The sensitivity study has shown that there is unlikely to be any margin for reducing the claimed C&I system reliabilities to more credible values without significantly increasing EDF/Areva's risk estimates to levels which are close to or in excess of the Basic Safety Levels (see HSE Safety Assessment Principles for Nuclear Facilities 2006 edition, Revision 1) (see Annex RI-UKEPR-2.A1). By way of comparison you should note that the claim on the Sizewell B computerised Primary Protection System (PPS) when standing alone was 10^{-4} pfd and for the most frequent faults the claim for the combination of the PPS and hardware (laddic) based Class 1 Secondary Protection System was 10^{-7} pfd. From this it can be seen that you are attempting to claim two orders of magnitude better reliability for the combination of two computer based systems (i.e. 10^{-9} pfd) one of which (i.e. the Siemens SPPA - T2000 platform) was (to our knowledge) not developed to nuclear sector protection system standards such as IEC 60880 or IEC 60987.

We have previously advised you that the provision of a hardware back up protection system (as employed in OL3) might be a possible way forward on some of the topics identified in this letter (see Annex RI-UKEPR-2.A1). The provision of a hardware backup system on OL3 and Class 1 display system (OL3 and US EPR) suggests that the implementation of such systems is reasonably practicable and necessary for a plant designed to meet modern international safety standards.

Further information on the RI and related draft Regulatory Issue Actions (RIAs) can be found in the Annex to this letter.

Please note we are sending a copy of this letter and its attachments to Mr Sylvain Petit at ASN. We also intend to provide a copy of this letter to our partners in the OECD MDEP EPR working group (i.e. US NRC, STUK and IRSN).

Please provide a response to this letter, including a plan for addressing the draft RIAs, by 22 May 2009. So that we can include consideration of your responses in our Step 3 report would you please ensure that you have completed all work necessary to address the RIAs and have provided us with a full response by the end of August 2009. In view of the complexity of some of the concerns linked to our draft RIAs please note that an acceptable full response in time for Step 3 (end August 2009) could be a conceptual design solution together with a plan and commitment to produce a detailed design solution during Step 4.

Yours sincerely

Nuclear Installations Inspectorate

References

1. IAEA safety guide NS-G-1.1 IAEA Safety Standards Series, Safety Guide No.NS-G-1.1 - Software for Computer Based Systems Important to Safety in Nuclear Power Plants. (2000).

2. IEC 61226:2005. Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.

3. Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2007

4. HSE T/TAST/046 Computer based safety systems.

5. Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units" adopted during plenary meetings of the GPR and German experts on the 19 and 26 October 2000.

6. The Tolerability of Risk From Nuclear Power Stations (HSE 1992) ISBN 0-11-886368-1.

7. The use of computers in safety-critical applications – Final report of the study group on the safety of operational computers – (HSC 1998) ISBN 0 7176 1620 7.

Annex

Regulatory Issue RI-UKEPR-2 - Draft Regulatory Issue Actions

RI-UKEPR-2.A1 – Adequacy of Reactor Protection System Arrangements.

Discussion - See letter for discussion related to this action. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE Safety Assessment Principles (SAPs); ECS.3 (O2)*, EDR.2 (O5), EDR.3 (O8), ERL.4, ESS.1, ESS.2 (O10), ESS.7 (O6), ESS.21 (O13), ESS.27 (O15) and ESR.5 (O16).

Action A1.1: EDF/Areva to review the UK EPR C&I systems' architecture to identify and implement measures to reduce the reliability claims placed on the Teleperm TXS and Siemens SPPA T2000 systems.

Action A1.2: EDF/Areva to review the UK EPR C&I systems' architecture to determine the reasonable practicability of providing a hardware based back up protection system (i.e. as provided on OL3, AP1000 and Sizewell B).

Action A1.3: EDF/Areva to demonstrate that the protection System PS (Teleperm XS) and back up/secondary protection system are adequately diverse and independent (ERC.2 (O7), ESS.18 and ESS.27/Ref. 4 Appendix 4).

Action A1.4: EDF/Areva to justify the reliability figures used for each of the protection systems when claimed independently and in combination. EDF/Areva to ensure its response includes consideration of appropriate guidance and standards (e.g. Refs 1 to 7) and explains how its standards reflect the functional reliability requirements. NB. UK research on high reliability computer based systems has shown that there are significant difficulties in justifying such systems.

Action A1.5: EDF/Areva to explain its approach to the demonstration of the adequacy of computer based systems important to safety (CBSIS) including the identification of production excellence and independent confidence building activities (Ref. 4) for each of the CBSIS.

RI-UKEPR-2.A2 – Failure Independence between Safety (Class 1) and Other Systems Including Safety Related Systems (Class 2/3).

Discussion - See letter (paragraph 2) for discussion related to this action. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ERC.2 (O7), ESS.15, ESS.18 and ESS.20.

Action A2.1: EDF/Areva to review and explain the extent of information transmitted to the Teleperm TXS Protection System from non F1A systems (e.g. permissives, vetoes and resets of automatically initiated F1 functions etc.).

Action A2.2:EDF/Areva to review and implement measures to ensure the C&I systems' design meets HSE SAP ESS 15, 18 and 20, and the security principle that there should be no communication to safety systems from safety related systems.

Action A2.3: EDF/Areva to demonstrate that electrical and functional isolation exists for interfaces to systems of different safety class.

Discussion – The Reactor Control, Surveillance and Limitation System (RCSL) and the protection system (PS) are both based on the Teleperm XS system and as such there exists the potential for a common mode failure of both systems.

Action A2.4: EDF/Areva to explain why the potential for common mode failure of the RCSL and PS is not a concern (SAP ESS 18).

RI-UKEPR-2.A3 – Provision of Class 1 Manual Controls and Indications in the MCR and RSS.

Discussion – There are no Class 1 manual controls or indications either in the MCR or RSS (c.f. AP1000 and Sizewell B which do have significant Class 1 manual controls and indications including hardwired reactor trip). Note that the SICS is Class 2 (F1B/E1B) and the interface to the Class 1 (F1A/E1A) protection system is via a communications bus (i.e. not hardwired). Manual operation of RT/ESFAS appears to be via the Class 3 (F2/E2) PAS. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ESS.3, ESS.8 and ESS.13.

Action A3: EDF/Areva to review the C&I architecture design to determine the reasonable practicability of providing Class 1 manual control and indication systems (e.g. as for the OL3 and US EPRs that have the TXS (QDS) which is not present in FA3 or UK EPR) in the MCR and RSS.

RI-UKEPR-2.A4 - EPR Function Categories and Equipment Classes

Discussion - EPR function categories do not appear to align with UK interpretation of IEC 61226 (see Table 1 below). The only agreement is for the PS and PACS (Category A) all others appear to be one category lower. EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ECS.1, ECS.2 and ECS.3.

Action: EDF/Areva to review Table 1 and provide the requested clarifications (see comments column of Table 1), namely;-

Action A4.1: EDF/Areva to clarify why the functional safety category of the SICS is not F1A.

Action A4.2: EDF/Areva to clarify the SICS operational state when the PICS is operational.

Action A4.3: EDF/Areva to review and explain the reasonable practicability of providing plant operation with indications and controls appropriate to the function (e.g. NSSS controls are normally Class 1/2 as per Sizewell B and AP1000) which are normally in operation as opposed to relying on changeover to a backup of correct class upon failure of the PICS.

Action A4.4: EDF/Areva to explain why the functions implemented in the SAS are not Category A (e.g. given implementation of reactor trip via the SAS).

Action A4.5: EDF/Areva to explain why the functions implemented in the RCSL are not Category B (e.g. given implementation of main reactor controls).

Action A4.6: EDF/Areva to explain whether the PAS implements any of the main reactor controls (e.g. reactor coolant temperature, pressuriser pressure/level, steam generator level, feed water and steam dump controls) and if so why Category B (F1B) is not the appropriate categorisation.

Action A4.7: EDF/Areva to explain how it determined that the SA I&C is Category C (F2).

RI-UKEPR-2.A5 - Network Determinism and Response Times

Discussion - Given the complexity of the architecture it appears that network determinism and response times may be an issue, for example to ensure that:-

- the time to acquire and display sensor information meets the required response times, and
- actuators can be operated within the required actuation times (i.e. including detection of the event requiring the actuation, subsequent information communication and signal and logic processing etc.).

EDF/Areva has not demonstrated that the UK EPR C&I design satisfies the following HSE SAPs; ESS.2 (FA9), ESS.5, ESR.2, ESR.3 and ESR.9.

Action A5: EDF/Areva to demonstrate that safety/safety related network communications are deterministic and the required response times are achievable (see examples in discussion above).

* NB. The references in brackets following identification of the SAPs in the above text are to Observations in HSE's Step 2 Report on EPR C&I.

Table 1

System	**Technology**	**Functional Safety Category** **EDF/AREVA**	**Safety Category** **NII – Based on BS IEC 61226**	**Comments**
Safety Information and Control System (SICS)	Mostly Hardwired but interface to PS is via PI/MSI/PS datalink.	F1B (B)	A	Requires clarification. - Need for Manual reactor trip/ESFAS actuation implies SICS should be Category A. SICS required to achieve and maintain safe state. SICS required to cover failure of PICS. EDF/Areva to clarify why the SICS is not F1A. EDF/Areva to clarify SICS operational state when PICS is operational.
Process Information and Control System (PICS)	SPPA-T2000	F2 (C)	B	Requires clarification. - PICS is the main control and operator station in the MCR and RSS, and is required to monitor and control plant in all plant conditions. Normal plant operation is with PICS Class 3 (F2) indications and controls. Changeover to the F1B SICs is required on failure of the PICS. EDF/AREVA argument for C is that B functions are backed up in the SICS. NII believes that Cat B functions should be delivered by operational equipment of the appropriate class NOT by changeover to a backup of correct class. EDF/Areva to review and explain the reasonable practicability of providing plant operation with indications and controls appropriate to the function (e.g. NSSS controls are normally class 1/2 as per Sizewell B and AP1000) which are normally in operation as opposed to relying on changeover to a backup of correct class upon failure of the PICS.
Protection System (PS)	TELEPERM XS	F1A (A)	A	Categorisation agreed.
Priority and Actuator Control System (PACS)	Mostly hardwired	F1A (A)	A	Categorisation agreed.
Safety Automation System (SAS)	SPPA-T2000	F1B (B)	A	Requires clarification. Implementation of diverse reactor trip function leads to Category A categorisation. EDF/Areva to explain why the functions implemented in the SAS are not category A (e.g. given implementation of reactor trip via the SAS).
Reactor Control, Surveillance and Limitation System (RCSL)	TELEPERM XS	F2 (C)	B	Requires clarification. - Main Reactor Controls, hence Category B function. EDF/Areva to explain why the functions implemented in the RCSL are not Category B (e.g. given implementation of main reactor controls).
Process Automation System (PAS)	SPPA-T2000	F2 (C)	B/C	Requires clarification. EDF/Areva to explain whether the PAS implements any of the main reactor controls and if so why Category B (F1B) is not the appropriate categorisation.
Severe Accident I&C (SA I&C)	TELEPERM XS	F2 (C)	B/C	Requires clarification. EDF/Areva to explain how it determined that the SA I&C is F2.