Office for Nuclear Regulation

An agency of HSE

Redgrave Court Merton Road Bootle Merseyside L20 7HS
Tel: 0151 951 4000 www.hse.gov.uk/nuclear

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**
GDA Issue	Absence of adequate C&I architecture. The proposal to address the issues raised in RI 02 includes provision of a hardware based backup system known as the NCSS. Detail of the NCSS design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA.		
GDA Issue Action	EDF and AREVA to provide a Basis of Safety Case (BSC) that includes substantiation of the design of the Class 2 Non-Computerised Safety System. An action plan for completion and supply of detailed evidence supporting the basis of safety case document should also be supplied. The BSC should consider: • The safety principles and standards (i.e. company, national and international) that EDF and AREVA has adopted for the NCSS. • The identification of arguments for assigning safety functions and performance requirements to the NCSS in compliance with these principles and standards. • The basis of the safety case should demonstrate how the safety principles and standards adopted have or will be complied with at each step of the development and deployment of the NCSS. • It should outline why the NCSS is considered to be fit for purpose and demonstrate how all of the safety principle, standards, functional and performance requirements will be satisfied. • It is expected that these demonstrations and examinations would identify the detailed evidence supporting the claims and arguments. • The BSC is also expected to identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification and link them to claims made and the demonstration of fitness for purpose of the systems. • It is expected that in undertaking this exercise compliance with ONR's SAPS would also be demonstrated with deviations justified. • The BSC should describe the system, breaking it down such that the major elements can be identified (such as input/output and logic cards). The BSC should include the demonstration of adequacy for each of these elements		

Redgrave Court Merton Road Bootle Merseyside L20 7HS
Tel: 0151 951 4000 www.hse.gov.uk/nuclear

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**

(including identification of revisions) as well as the NCSS as a whole.

- The BSC should set down the production excellence arguments and identify the independent confidence building measures.
- The BSC should describe the project QA arrangements, e.g. ISO 9001, this should include a clear description of the interface to the NCSS supplier (and any other suppliers). The BSC would also be expected to outline the NCSS supplier QA arrangements.
- The BSC should identify the pedigree of any COTS, pre-developed components as this might influence how they are justified for use.
- The BSC should demonstrate that the management arrangements for COTS/pre-developed components has been and remains adequate. This demonstration should cover, amongst others, configuration management, collection of Operating Experience and any changes along with their cause and how the change was implemented (capturing the evolution of the QA regime and processes by which this has been done).
- The BSC should address the process by which the individual components will be brought together and integrated as a system. It is anticipated this would be detailed in the BSC (or other documents referenced from the BSC) covering factory and commissioning testing as well as environmental qualification work that might be called upon to support system justification. For completeness, it should also address through life operating and maintenance, for example identifying the scope and frequency of any proof testing that is required.
- Should elements of the implementation of the NCSS system make use of complex electronic devices e.g. FPGAs (but not microprocessors) then the basis of the safety case would be expected to demonstrate how the design and implementation of the NCSS complies with relevant EDF/Areva safety principles and standards. The basis of safety case should also identify how ND guidance, for example, that contained in ESS.21 which requires the safety demonstration to include measures such as independent third party assessment (para. 355) will be addressed. Given the programmable nature of such complex devices, the justification should draw on elements of ESS.27 and the special case procedure with an argument of excellence in production and independent confidence building in respect of the systems fitness for purpose. It is expected, as above, that the demonstration would identify the detailed evidence supporting the claims

Office for Nuclear Regulation

An agency of HSE

Redgrave Court Merton Road Bootle Merseyside L20 7HS
Tel: 0151 951 4000 www.hse.gov.uk/nuclear

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**
	and arguments made. For further guidance see also T15.TO1.46 in Annex 5, T16.TO1.02 in Annex 6, T17.TO1.24 in Annex 7 and T20.A1.2.4 in Annex 9 of Step 4 C&I Division 6 Assessment Report, No. 11/022 Revision A (DRAFT). With agreement from the Regulator this action may be completed by alternative means.		