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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A1**
GDA Issue	In response to our assessment, EDF and AREVA have agreed architecture changes, categorisation changes and have committed to develop a programme of Independent Confidence Building Measures to support the EPR C&I safety case. The nine actions under this GDA issue are concerned with C&I architecture and related matters.		
GDA Issue Action	EDF and AREVA to provide a comprehensive justification of diversity and independence between NCSS/PS, NCSS/SAS-PAS and PS/SAS-PAS commensurate with the level of design for a pre-construction safety report. One of the C&I architectural changes introduces in response to RI02 was the addition of a Non-Computerised Safety System as a backup to the computer- based Safety Automation System/Process Automation System and the Protection System. The EDF and AREVA safety case claims diversity and independence between each of these systems, however, this claim has not been fully substantiated. The regulator expects that this detailed diversity analysis will draw on appropriate standards and guidance. It is also expected that this analysis will be rigorous and ensure all common components are identified together with argumentation as to why any such components identified do not have the potential to induce Common Cause Failure of the identified systems. Where final detailed design information is not available, but which is identified has having a potential impact on the diversity analysis, this should be noted and ONR will use the vehicle of an assessment finding to track the gathering of this evidence from a future licensee. For further guidance see also T13.TO1.04 in Annex 3, T16.TO2.21 in Annex 6, T18.TO1.03, T18.TO1.04 and T18.TO2.09 in Annex 8 and T20.A1.2.3 and T20.A1.3.4 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	**PSA** **Structural Integrity**		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A2**
GDA Issue Action	EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The response should include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards. The EDF and AREVA safety case makes a claim of $1x10^{-4}$ probability of failure on demand (pfd) for the Class 1 Protection System (PS), $1x10^{-2}$ pfd for the Safety Automation System (SAS) and $1x10^{-3}$ pfd for the Non-Computerised Safety System (NCSS). However, a justification for each of these figures needs to be provided, for example, drawing on appropriate international standards (covering random and systematic failures). In addition, for the claims to be used in a way which allows their multiplication, additional argumentation will be required (e.g. claims of independence and diversity which will need to be substantiated) – see GI-UKEPR-CI-06.A1. For further guidance see also T16.TO2.21 in Annex 6, and T20.A1.4.1 and T20.A1.4.2 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A3**
GDA Issue Action	EDF and AREVA to provide a justification of the approach to be used to demonstrate the adequacy of computer based systems important to safety including identification of production excellence and independent confidence building activities. SAP ESS.27 requires that where a safety system's reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures. Note that the Protection System's independent confidence building measures are to be addressed under GI-UKEPR-CI-03. For further guidance see also T20.A1.4.1.a 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A4**
GDA Issue Action	EDF and AREVA to provide a revised document NLN-F DC 193 'Protection System – System Description' to reflect the current design and to provide full justification for the design, including the justification of hardwired links to the PS. The assessed revision of NLN-F DC 193 does not reflect agreed architectural changes and does not provide justification for all the hardwired links from lower class systems to the Class 1 Protection System (noting that there may be detailed implementation issues which cannot be fully addressed under GDA). For further guidance see also T17.TO1.04 in Annex 7, T20.A2.2.1 and T20.A2.2.3 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A5**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of independence between PICS Class 3 and SAS Class 2 systems. EDF and AREVA to provide detailed substantiation of independence between Process Instrumentation and Control System (PICS) Class 3 system and the Safety Actuation System (SAS) Class 2 system. There are data highway based communications from the Class 3 to the Class 2 system and EDF and AREVA are required to provide detailed substantiation that failure of the lower class system cannot compromise operation of the higher class system. For further guidance see also T20.A2.3.2 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A6**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of the Class 1 control and display facilities to be provided in the MCR and RSS. A Basis of Safety Case for the Class 1 control and display system to be provided and also a justification in terms of the functional coverage of this system. In response to our assessment a number of C&I architectural changes were introduced to eliminate network communications from lower class systems to the Class 1 protection system, and one such change was the introduction of Class 1 control and display panels in the Main Control Room and the Remote Shutdown Station. EDF and AREVA has indicated that the arrangements will be enhanced by provision of a Qualified Display System (QDS). However, the proposed technical solution, and the scope of the displays/controls needs to be confirmed. For further guidance see also: T16.TO1.03 in Annex 6; T17.TO1.14, T17.TO1.15 and T17.TO2.16 in Annex 7; and T20.A3.6 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A7**
GDA Issue Action	EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. Normal control is through use of the PICS controls with a switch mechanism used to activate the SICS controls on detection of PICS failure. EDF and AREVA is to describe the arrangements used for this changeover including detection of PICS failure. The SICS displays remain active but the audible alarms are muted. The description to be provided by EDF and AREVA will include an argument as to why leaving the SICS controls inactive until needed following PICS failure is preferable to having them active. With agreement from the Regulator this action may be completed by alternative means.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A8**
GDA Issue Action	EDF and AREVA to provide evidence, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design. EDF and AREVA have yet to provide adequate substantiation to confirm that performance is guaranteed by design for those functions which use the Class 3 Terminal bus and/or Plant bus with respect to the end-to-end response time. For further guidance see also T20.A5.4 and T20.A5.5 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.		

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

ISSUES ARISING FROM RI02

GI-UKEPR-CI-06 REVISION 3

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		**PSA** **Structural Integrity**	
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A9**
GDA Issue Action	EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection e.g. sensors, smart devices, PIPS, PACS (response to include consideration of the potential for common mode failure as a result of the use of these components). A comprehensive analysis should be provided by EDF and AREVA to address the potential for Common Cause Failure due to the use of common components in different nominally diverse systems. Also to address the use of items used to provide inputs to more than one line of protection, such as PIPS, and items which combine outputs from nominally diverse/independent systems such as the PACS. For further guidance see also: T17.TO2.07, T17.TO2.08 and T17.TO2.28 in Annex 7; T18.TO1.02, T18.TO1.05 and T18.TO2.06 in Annex 8; T20.A1.3.1 and T20.A1.3.5 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.		