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

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DCIS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A1**
GDA Issue	The AP1000 automatic controls and its manual controls and displays are in the DCIS (PLS/DDS). The systems have to be justified as Class 2 (PLS) and Class 3 (DDS) respectively as part of the plant safety case; this requires a new justification as the systems are given a non safety classification in the US. The justification is expected to be in the form of a basis of safety case supported by documented evidence substantiating the claims for the systems and their development. For further guidance, see T15.TO2.36 in Annex 5 and T16.TO1.05 and its associated TO2s, and T16.TO2.19 to 27 in Annex 6 of ONR C&I Assessment Report No. 11/006 (draft).		
GDA Issue Action	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PLS and DDS applications. 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

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DCIS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A2**
GDA Issue Action	Westinghouse to provide a basis of safety case that includes a justification of the suitability of the PLS application at Class 2 (control) and the DDS application at Class 3 (manual control and display). The content of a BSC is outlined below. The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques.		

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

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DCIS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A2**
	The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration. The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, SAP ESS.27 a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.		