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

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A1**
GDA Issue	Shortfalls have been identified in the provision of a claims - argument - evidence structure in the CIM safety case. The CIM is a critical component of the primary protection system. It is based on Field Programmable gate array (FPGA) technology and is supplied by a company with little experience in the nuclear sector. In response to our concerns WEC has produced a Basis of Safety Case (BSC) for the CIM. Assessment of the BSC has identified a number of areas for improvement. The key areas for improvement are: • demonstration that the development process is compliant or equivalent to IEC standards; and • identification of the evidence to support the demonstration. The BSC should document the standards compliance and address issues related to use of tools and test coverage. The rigour of the safety demonstration provided in the BSC should reflect the reliability claim on the CIM. The CIM safety case needs to incorporate the responses to the CIM related Assessment Findings identified in ONR C&I Assessment Report No. 11/006 (draft) and to reflect CIM development progress as the design is completed. For further guidance, see T15.TO1.05, T15.TO1.06, T15.TO1.07, T15.TO1.08, T15.TO1.10 and their associated TO2s in Annex 5 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 CIM. 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

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A2**
GDA Issue Action	Westinghouse to provide the basis of safety case for the completed design of the CIM. The expectation is that the observations already provided will be taken into account along with those in the ONR GDA Step 4 report and in particular account will be taken of the remedial action including IV&V undertaken by Westinghouse. The detailed evidence above will be assessed as part of the CIM BSC review. The expectations of the form and a basis of safety case for the CIM are set down 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,		

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

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A2**

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.

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; and
- prototype equipment has been produced and subject to performance and qualification testing.

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

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area		**CONTROL AND INSTRUMENTATION**	
Related Technical Areas		None	
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A2**
	With agreement from the Regulator this action may be completed by alternative means.		