

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

DIVERSITY OF PLS, PMS (INC CIM) AND DAS

GI-AP1000-CI-03 REVISION 0

Technical Area		CONTROL AND INSTRUMENTATION	
Related Technical Areas		None	
GDA Issue Reference	GI-AP1000-CI-03	GDA Issue Action Reference	GI-AP1000-CI-03.A1
GDA Issue	<p>ONR identified an apparent lack of diversity of the primary protection system PMS (the CIM) and the diverse secondary protection system DAS. Diversity between the PMS (CIM) and DAS was a significant issue as it was proposed to use the same FPGA component suppliers and application developers. The change of choice of DAS platform to a conventional discrete electronic one provided a significant step forwards. Nevertheless a detailed diversity analysis is required for the DAS against the PLS/DDS and the PMS. ONR's expectation is that these diversity analyses will be set out in an appropriate basis of safety case.</p> <p>For further guidance, see T18.TO1.01, T18.TO2.06, T18.TO2.11, T18.TO2.19, T18.TO2.21 and T18.TO2.25 in Annex 8 of ONR C&I Assessment Report No. 11/006 (draft).</p>		
GDA Issue Action	<p>Provide a detailed diversity analysis for the DAS (7300 series) against the PLS/DDS (Ovation) and the PMS (Common Q).</p> <p>Defence against failure of the control system PLS (and others such as the TOS) is provided by the PMS primary and DAS secondary protection systems; further, defence against PMS failure is provided by DAS. In order for such defences to be effective the systems need to have properties including independence and diversity. The diversity of the PMS's CIM component and the DAS was raised a number of times and challenged as the CIM and DAS were to be implemented: by the same application developer; in the same FPGA technology, and using FPGAs and development tools from the same supplier. In response Westinghouse advised that the technology choice for the DAS would be changed to use its 7300 series equipment based primarily on analogue technology. This was seen as a significant step forward; however, once the DAS and PLS designs are complete a detailed diversity analysis will be required for the PMS and DAS and for the PLS and DAS.</p> <p>Note the analysis should be included in a basis of safety case document, for example, that for the DAS. The revised DAS technology choice to be formally introduced, its design completed to allow the necessary detailed diversity analysis to be completed to substantiate that it is diverse from both the PLS/DDS and PMS.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		