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
USE OF THE BEACON CODE FOR ON-LINE COMPLIANCE
GI-AP1000-FD-03 REVISION 0

Technical Area		**FUEL DESIGN**	
Related Technical Areas		Fault Studies	
GDA Issue Reference	**GI-AP1000-FD-03**	**GDA Issue Action Reference**	**GI-AP1000-FD-03.A1**
GDA Issue	Provide a safety case to demonstrate compliance with the fuel and fault study limits in the event of an unrevealed failure of the BEACON code.		
GDA Issue Action	Identify the processes in which BEACON contributes directly or indirectly to nuclear safety and the hazards that arise should the BEACON software act in a malignant manor. Evaluate by fault studies the risk associated with each failure sequence and demonstrate that no further measures to mitigate the risk of BEACON failure are reasonably practical. While significant effort has been made to demonstrate that BEACON is a useful and reliable tool, these arguments are only of limited use. While reliance is placed on the correct functioning of a system, a high safety classification is indicated and this may not be reasonably achievable. The NII safety assessment principles advise that design basis analysis should provide an input into safety classification and the requirements for systems providing a safety function. Accordingly, a safety case must address the consequences of the software failing or an unrevealed failure becoming apparent during a fault. The safety analysis process for BEACON should be similar to the consideration of failure in any other system i.e. it should examine potential hazards and ultimately quantify risk. ONR expects a detailed justification that the processes in which BEACON is used are robust against BEACON failure in normal operation and in simultaneous faults and that risk is ALARP. Usually acceptable mitigation of faults can be claimed if an independent means exists for the operator to verify that the reactor remains compliant with the safety case and that these are likely to be used on a frequency determined by the risk assessment. With agreement from the Regulator this action may be completed by alternative means.		