Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-FD-03
Use of the BEACON Code for On-line Compliance

MAIN ASSESSMENT AREA	RELATED ASSESSMENT AREA(S)	RESOLUTION PLAN REVISION	GDA ISSUE REVISION
Fuel and Reactor Core	FS,HF,CI	3	0

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.
ACTION: GI-AP1000-FD-03.A1	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.

RELEVANT REFERENCE DOCUMENTATION RELATED TO GDA ISSUE	
Technical Queries	
Regulatory Observations	
Other Documentation	WEC70123R, "Regulatory Observation RO-**AP1000**-49 and Regulatory Observation Action RO-**AP1000**-49.A1.1 – Use of the BEACON Code for On-line Compliance with Technical Specifications" WEC70212R, "Westinghouse Response to RO-**AP1000**-40 and RO-**AP1000**-049.A2.1 – Use of the BEACON Code"

Scope of work:

In order to address this GDA issue, Westinghouse will develop a complete safety case for the implementation of the BEACON system, as intended for the **AP1000**® plant design.

Description of work:

Following the expected claims, arguments, evidence format, the safety case will include the following:

- Identify the processes in which the BEACON system contributes directly or indirectly to nuclear safety.
  - The BEACON system provides surveillance of initial conditions assumed as input into certain safety analysis. The evaluation will document where these inputs are assumed in the Westinghouse safety analysis. In addition to surveillance functions the BEACON system could be used for predictive and diagnostic purposes. These uses as well as any credible uses outside of the design intent of the BEACON system will be considered.
- Identity the hazards should the BEACON system present the end user with data that does not accurately represent the conditions in the core and evaluate the consequences to the safety analysis.
  - The hazards analysis will consider cases where the BEACON system indicates a need for administrative action when no action is required, as well as when the BEACON system indicates no administrative action is required but in reality some action should be taken. Current safety systems will be taken credit for in the determination of the initial conditions (e.g. PMS f(mpact of the BEACON system on interfacing systems as a result of physical connection to the Ovation network, or data being passed from the BEACON system to another plant system. ips, et
- Evaluate further measures to mitigate the risk of a BEACON system failure.
  - An ALARP assessment of the BEACON system will evaluate the current surveillances, available plant parameters, and available off-line

calculations or evaluations to determine if additional measures are necessary to support validation of the proper functioning of the core monitoring performed by the BEACON system.

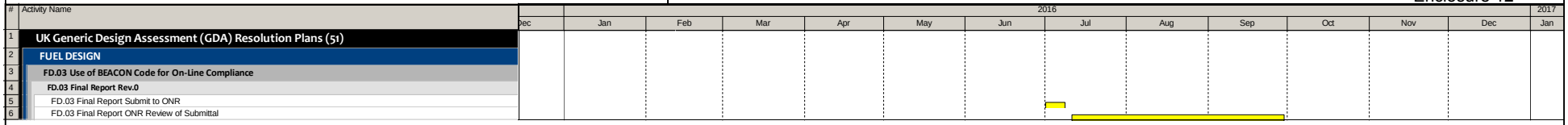
- The previously identified analysis and findings of the ALARP assessment will be documented in a safety case for the BEACON system.

Deliverables:

- BEACON System Safety Case

Schedule/ programme milestones:

Please see the following page for the detailed schedule.



Methodology:
No new methodologies will be utilised to resolve this GDA issue.

Justification of adequacy:
The final safety case will demonstrate that the implementation of the BEACON system in the **AP1000** plant design, for both core monitoring and operational predictions does not result in an increase in risk to the operation of the plant and is a net benefit to the plant design. The process outlined for developing the safety case engages the ONR throughout the development process in order to provide high confidence that the final developed safety case will satisfactorily resolve the current GDA issue.

Impact assessment:
No previously submitted documents are expected to be impacted by this work.