New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-FD-03
BEACON Core Monitoring System Justification

Assessment Report: ONR-NR-AR-16-008
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

Westinghouse Electric Company LLP is the reactor design company for the **AP1000**® reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to the award of a Design Acceptance Confirmation (DAC) and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report is part of the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fuel design. Specifically, this report addresses GDA Issue GI-AP1000-FD-03: BEACON™ Core Monitoring System Justification.

This GDA issue arose in Step 4 due to the proposed use of the BEACON core monitoring system to support safety functions important to safety, despite the system not being qualified to meet the requirements of the appropriate UK safety class.

The Westinghouse GDA Issue Resolution Plan stated that its approach to closing the issues was:

- to provide a justification of the system as broadly compliant with the requirements of a Class 3 safety system;
- to identify the 'failure modes and effects' for the BEACON system and then changes to the design and operation of the system, to minimise the impact of faults.

My assessment conclusions are:

- Westinghouse has made sufficient changes to operating procedures to reduce the risk associated with potential failures of the BEACON system As Far As Reasonably Practicable (ALARP).
- The BEACON core monitoring system is therefore acceptable in principle for use in the UK **AP1000** reactor.
- It is acceptable that detailed design justification will be made when the system hardware is known.

My judgement is based upon the following factors:

- Westinghouse has completed a failure modes and effects analysis and has included changes to operating procedures to reduce the safety impact of the BEACON system.
- Westinghouse has introduced diverse checks on protection system operating parameters derived from BEACON data.
- Westinghouse has made an initial justification of the adequacy of the BEACON system to meet the expectations of a Class 3 safety system and this will be repeated when the design of the system hardware is finalised.

The following matters remain, which are for a future licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic safety submission and do require licensee input / decision.

The BEACON system runs on a Linux computer and is therefore potentially subject to issues of obsolescence. Westinghouse will update the design before installation and a future licensee needs to account for this. The current design justification is therefore preliminary and will need to be repeated at an appropriate time during construction to reflect the available technology. This is captured in an assessment finding as follows:

> "Westinghouse has carried out an assessment of the adequacy of the generic BEACON system to demonstrate that it meets the production excellence requirements for a Class 3 system. This has included verification of the software design against current standards and an assessment of failure modes. However, the licensee will

> need to repeat this assessment of production excellence when the plant-specific system design and hardware have been identified."

In summary, I am satisfied that GDA Issue GI-AP1000-FD-03 can be closed.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
BSL	Basic Safety Level
C&I	Control and Instrumentation
CASE	computer-aided software engineering
DDS	**AP1000** Data Display and Processing System
GDA	Generic Design Assessment
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IIS	**AP1000** Incore Instrumentation System
LowSIL	Low Safety Integrity Level
ONR	Office for Nuclear Regulation
OPDMS	Online Power Distribution Monitoring System
PCSR	Pre-construction safety report
PLS	Plant Control System
PMS	Protection and Safety Monitoring Systems
RGP	Relevant Good Practice
RP	Requesting Party
SAPs	Safety Assessment Principles
SSC	Structure, System and Component
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
US NRC	United States (of America) Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

Annex

1 INTRODUCTION

1.1 Background

1. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and then paused the regulatory process. It achieved an Interim Design Approval Certificate (IDAC) which had 51 GDA issues attached to it. These issues require resolution before the award of a DAC and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

2. This report is part of ONR's assessment of the Westinghouse **AP1000** reactor design in the area of fuel design. Specifically, this report addresses GDA Issue GI-AP1000-FD-03 – BEACON© Core Monitoring System Justification.

3. The related GDA Step 4 report is published on our website (www.onr.org.uk/new-reactors/ap1000/reports.htm), and this provides the assessment underpinning the GDA issue. Information on the GDA process in general is also available on our website (www.onr.org.uk/new-reactors/index.htm).

4. As part of the **AP1000** design, Westinghouse introduced a software tool called BEACON to assist operators. This included a model of the reactor core and the associated instrumentation. The tool can provide a high precision representation of the state of the core and can predict the outcome of proposed operator actions. It allows surveillance of more fundamental core parameters – such as safety margins to the critical heat flux and the shutdown margin.

5. As part of GDA, I noted that the BEACON system appeared to be used to make a significant contribution to the success of the reactor protection system in faults, yet it had no safety classification.

6. Safety classification is used to ensure that a system is designed and constructed to meet the appropriate level of reliability, to ensure that the claims made on the safety function can be supported. I judged that the BEACON system was too complex to meet the level of reliability I expected for certain of the safety functions proposed. I therefore raised a GDA issue, intended to ensure that the assumptions used in the fault studies remain valid. The issue required Westinghouse to:

> 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.

7. Westinghouse's response to this issue was to argue 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.

8. The basis of its safety case has been documented in a series of claims which are derived from an analysis of: the functions to which the BEACON system contributes; likely modes and effects of failure; and the compliance of the system with appropriate design standards.

9. This report assesses the arguments presented and the associated evidence to determine whether the submission supports an adequate safety case for the use of the BEACON system in the UK **AP1000** reactor.

1.2 Scope

10. In raising the GDA issue, ONR required Westinghouse to 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.

11. The scope of this assessment is detailed in the assessment plan (Ref. 1). I have focused on the adequacy of the optioneering and the selection of measures identified to prevent and mitigate the effect of errors in the operation of the BEACON system. This has been examined from a fault-analysis perspective. The detailed design has been examined at a high level to determine whether there are any serious shortcomings that would prevent acceptance of the system.

12. Confirming a proof of concept is adequate at this stage given the need to carry out more detailed analysis of the specific hardware at a later date.

1.3 Method

13. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 2).

1.3.1 Sampling strategy

14. It is rarely possible or necessary to assess a safety submission in its entirety, and therefore ONR adopts an assessment strategy of sampling.

15. I have examined the analysis of potential system failure modes and effects and the optioneering necessary to determine which additional measures are reasonably practical.

16. I have sampled the qualification of the BEACON system against standards for control systems important to safety and assessed this based on my experience of software development. However, specialist assessment by control system engineers has not been carried out during GDA. This area has not been targeted for detailed assessment due partly to the fact that the system will use computers that are commercially available at the time of construction. As a result, Westinghouse will repeat its analysis for the specific hardware identified at the time, in consultation with the licensee.

17. Unrevealed failures in the BEACON system have the potential to mislead the operators in their response to faults and this has been addressed to an extent in the submission. However, this is best explored by use of a full-scope simulator. The human factors specialist assessor is content to address any outstanding issues as part of wider assessment findings on control-room design. I have therefore not sampled this aspect.

18. This sampling approach is also informed by the need to focus available resource, in the control and instrumentation topic area, on systems of higher safety significance. Complex core monitoring systems are employed on existing reactors and are therefore not a concern in principle and there will be opportunities to assess the detail of the design as it develops.

19. The scope of assessment is appropriate for GDA because I judged that the most effective means of reducing the risk associated with this system is to minimise reliance on the system by providing additional provisions and this aspect has been addressed.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

20. ONR's GDA Guidance to Requesting Parties (www.onr.org.uk/new-reactors/ngn03.pdf, Ref. 3) states that the information required for GDA may be in the form of a PCSR, and Technical Assessment Guide (TAG) 51 sets out regulatory expectations for a PCSR (www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf).

21. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the **AP1000** design reference point.

22. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, and therefore this report does not discuss the fuel design aspects of the PCSR. This assessment focused on the supporting documents and evidence specific to GDA Issue GI-AP1000-FD-03.

2.2 Standards and Criteria

23. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) (Ref. 5), internal TAGs (Ref. 6), relevant national and international standards and Relevant Good Practice (RGP) informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

24. The key SAPs applied within the assessment are included within Table 1.

Table 1: Relevant Safety Assessment Principles

SAP Number	SAP Title	Notes
EKP.1	Inherent safety	The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility
EKP.2	Fault tolerance	The sensitivity of the facility to potential faults should be minimised
EKP.3	Defence-in-depth	A nuclear facility should be so designed and operated that defence-in-depth against potentially significant faults or failures are achieved by the provision of several levels of protection
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety
ERC.1	Design and operation of reactors	The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor
ERC.2	Shutdown systems	At least two diverse systems should be provided for shutting down a civil reactor

Table 1: Relevant Safety Assessment Principles

SAP Number	SAP Title	Notes
ERC.3	Stability in normal operation	The core should be stable in normal operation and should not undergo sudden changes of condition when operating parameters go outside their specified range
ERC.4	Monitoring of safety-related parameters	The core should be designed so that safety-related parameters and conditions can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected
ERL-	Reliability claims	Measures to achieve reliability
ESS.27	Computer-based safety systems	Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design
ESR.10	Demands on safety systems in the event of control system faults	Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on safety systems or take any safety system beyond its capability limits
EMT-	Maintenance, inspection and testing	Identification of maintenance and testing requirements
FA-	Validity of data and methods	Theoretical models and calculation methods

2.2.2 Technical Assessment Guides (TAGs)

25. The following TAGs have been used as part of this assessment (Ref. 6).

Table 2: Relevant Technical Assessment Guides

TAG Number	TAG Title	Notes
NS-TAST-GD-005	Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)	Adequacy of safety measures
NS-TAST-GD-94	Categorisation of Safety Functions and Classification of Structures, Systems and Components	Identification of the safety category of safety functions required for fault tolerance and the classification of systems required
NS-TAST-GD-031 Revision 4	Safety Related Instrumentation	Safety requirements for low Safety Integrity Level (LowSIL) systems
NS-TAST-GD-075	Safety of Nuclear Fuel in Power Reactors	Requirements on the fuel and core
NS-TAST-GD-034 Revision 2	Transient Analysis for DBAs in Nuclear Reactors	Requirements for deterministic analysis of postulated faults

2.3 National and International Standards and Guidance

26. The national and international standards and guidance that have been used as part of this assessment are set out in Table 3. The standards relating to production excellence are British versions of international standards (Ref. 9) and the detailed good practice relating to safety analysis is found in guidance developed by international bodies to which ONR is committed (Refs 7 and 8).

Table 3: Relevant Standards

Reference	Title	Notes
SF-1	Fundamental Safety Principles	Safety principles
NS-R-1	Safety of Nuclear Power Plants: Design, Specific Safety Requirements	General requirements
NS-G-1.12	Design of the Reactor Core for Nuclear Power Plants	Specific design requirements
BS EN 61226 2010	Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions	Classification of safety systems
IEC 62138	Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions	International Electrotechnical Commission (IEC) Design standards for Class 3 systems
WENRA	WENRA Safety Reference Levels for Existing Reactors	Specific design requirements

2.4 Use of Technical Support Contractors (TSCs)

27. It is usual in GDA for ONR to use technical support, for example to provide additional capacity to optimise the assessment process, to enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision-making and so on. However, in this case, I felt that it was unnecessary to seek external advice.

2.5 Integration with Other Assessment Topics

28. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues of a multi-topic or cross-cutting nature. The following cross-cutting issues have been considered within this assessment.

29. Consideration of the impact of faults in the BEACON system on the plant's tolerance of faults required interaction with fault studies.

30. The interaction of the BEACON system with the operator required interaction with the human factors expert.

31. Demonstration of compliance of the BEACON system with the requirements for systems important to safety required interaction with experts in control and instrumentation.

3 REQUESTING PARTY'S SAFETY CASE

32. The Westinghouse safety case for GDA Issue GI-AP1000-FD-03 is documented in Ref. 10. Detailed analysis of the consequences of faults in the BEACON system is reported in Ref. 14 and the consideration of reasonably practical safety enhancements is documented in Ref. 12. Analysis of the impact on operator reliability is presented in Ref. 17.

3.1 BEACON Core Monitoring System Context

33. BEACON is not a standalone system; for the **AP1000** plant, it resides within the Incore Instrumentation System (IIS), which interfaces with the Data Display and Processing System (DDS). These Class 3 systems, and others, form the monitoring portion of the **AP1000** plant Control and Instrumentation (C&I) Systems.

34. The automatic control of the plant is discrete from monitoring. It is performed by the Class 2 Plant Control System (PLS).

35. The primary safety functions are also separate and are the responsibility of the Class 1 Protection and Safety Monitoring Systems (PMS).

36. The **AP1000** plant C&I architecture and systems are described in more detail in Chapter 19 of the **AP1000** PCSR (Ref. 16).

37. The BEACON instrumentation is inserted into the active core through the reactor pressure vessel upper head and internals of the vessel. Signals output from fixed in-core detectors are digitised inside containment and multiplexed out of the containment. The signal-processing software then calculates a precise 3-D core power distribution, suitable for calibration of the ex-core nuclear instrumentation, which is part of the reactor protection system.

38. The calibration information is developed using the BEACON core monitoring system and then confirmed via the DDS. The BEACON system is also capable of determining whether the reactor power distribution is within the operating limits defined in the plant operating rules (Technical Specifications).

39. The BEACON core monitoring system provides online monitoring of margins to thermal and shutdown-margin limits defined by Technical Specifications for the **AP1000** plant.

40. The BEACON system also provides alarms in the control room via the DDS.

3.2 System Classification

41. Westinghouse claimed that these functions are either Category C or Category B, but BEACON is not the only system delivering the function. Consequentially, Westinghouse argued that it is acceptable to design the system against Class 3 requirements; in accordance with IEC 61226, "Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions" (Ref. 9). This is based on an analysis of the safety functions provided by the BEACON system and a failure modes and effects analysis to determine the safety impact of BEACON system failure. The approach to system justification adopted by Westinghouse is summarised below:

- Determine the safety analysis items that could be affected if the BEACON system is providing erroneous results.
- Review the current safety analysis for the affected items to determine if mitigation measures are currently in place.

- For safety analysis events where the erroneous BEACON system scenario is not mitigated by measures currently in place, determine the safety-related consequence.

42. The analysis concluded that the consequences of each of the identified events were within the limits of the safety analysis. Furthermore, the BEACON system design meets the requirements of a Class 3 system as defined in IEC 62138 (Ref. 9).

3.3 Design Substantiation

43. Westinghouse argued that the BEACON system meets appropriate levels of production excellence (in accordance with SAP ESS.27) by compliance with C&I standard IEC 62138.

44. Westinghouse provided arguments justifying the adequacy of the BEACON software in the following areas:

- function and performance (ie safety functions to be performed and required response time)
- defence-in-depth (ie echelons of defence against common-cause failure of BEACON elements)
- interfaces between modules and hardware elements
- environmental qualification
- internal and external hazards and
- operation and maintenance.

45. Documentation was provided for each of these topics to demonstrate compliance with standards and/or to identify planned improvements.

3.4 ALARP Risk Reduction Measures

46. Westinghouse carried out optioneering to determine whether there are any additional measures that can be taken to enhance the safety performance of the BEACON system and to reduce the safety impact of potential BEACON failure. Westinghouse argued that the BEACON system design (as implemented in the **AP1000** plant) has reduced risks As Low As Reasonably Practicable (ALARP) (Ref. 12).

47. Westinghouse identified three design changes which were intended to reduce the plant's reliance on the BEACON system to carry out category B safety functions (Refs 13 and 14).

Change 1: Confirmation of Calibration

48. Westinghouse proposed incorporation of a new Nuclear Application Program to confirm correctness of the power-range ex-core calibration factors calculated by the BEACON system. This function will allow operators to enter the ex-core calibration factors and see the result of applying those factors to the signals from the ex-core channels. This will allow confirmation of the acceptability of the calibration factors used in the determination of weighted peripheral Axial Flux Difference before they are entered into the PMS.

49. The procedure for doing this will include constraints on the magnitude of changes permitted between successive calibrations.

Change 2: Applicability of Power-distribution Limits

50. Removal of the 'with [Online Power Distribution Monitoring System] OPDMS not functional' clause from the applicability of Limiting Condition for operation in Technical Specification 3.2.3 ensures that the rules will be applicable regardless of BEACON system functionality.

51. This reduces reliance on the BEACON system for confirmation of acceptable operating margin and ensures adequate fault tolerance in this respect irrespective of the functioning of BEACON.

Change 3: Boration Requirements

52. The Nuclear Design and Core Management Report for UK **AP1000** units will need to include sufficient information to allow reactor engineers to confirm that adequate shutdown margin is maintained during shutdown modes. This function is available in the BEACON system in the standard **AP1000** plant. However, to meet UK regulatory expectations, the necessary data should be provided to station staff as part of the reload justification, to allow them to perform their own determination of required soluble boron concentration requirements outside of the BEACON system.

53. The procedures will need to be revised to accommodate UK-specific surveillances and hand-created calculation of the shutdown-margin boron concentrations.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-FD-03

54. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 4).

4.1 Scope of Assessment Undertaken

55. The scope of the assessment is detailed in Section 1.2 above. My expectations are informed by the SAPs in relation to safety systems, which advise that adequate provisions should be made to enable the monitoring of the facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions.

56. Moreover, the SAPs advise that important Structures, Systems and Components (SSCs), including software for instrumentation and control, are classified based on their safety significance as determined by the fault analysis of the facility; then that all SSCs are designed, manufactured, installed and subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.

4.2 Assessment

57. My assessment firstly considered the following aspects of the safety justification:

- safety functions required of the system and the appropriate level of safety classification;
- measures that could reduce the consequences of BEACON system faults to reasonably practical levels; and
- measures taken to demonstrate system ‘production excellence’ by comparison with relevant standards (although this has been limited at this stage in the design process).

4.2.1 System classification

58. The BEACON system provides online monitoring of core parameters which need to be maintained within limits to ensure adequate fault tolerance.

59. In my experience, UK and international RGP is to limit these parameters by the plant Technical Specifications and to monitor the plant by information supplied from (at least) a Class 2 safety system. However, during Step 4 of GDA, Westinghouse proposed to use the BEACON system. BEACON can ensure compliance to greater precision; allowing relaxed operating limits (but at a lower reliability). I challenged this in a series of meetings and correspondence (for example, TQ-AP1000-559) because I took the view that some of the proposed surveillances are particularly important. The required boron concentration to provide adequate shutdown margin is a particular case where compliance is essential to providing the necessary fault tolerance.

60. Westinghouse agreed that the BEACON system could not meet the system reliability required by the UK classification system if it was the primary means of achieving these safety functions. It therefore reinstated compliance monitoring using the conventional parameters from the PMS, using the Technical Specification surveillances applied in previous Westinghouse designs. I am content with the proposed surveillances in principle.

61. The BEACON system can provide detailed information to the operator related to the axial and radial distribution of power. Furthermore, the BEACON system includes a

suite of functions that will be used by trained and qualified personnel to provide reactivity management guidelines for operation of the reactor.

62. I judged that these functions are desirable and provide a significant safety benefit, but since they contribute to safety, I needed to consider whether Westinghouse has demonstrated that the system is adequately reliable. The requirements of SAP ECS.2 apply:

> *"Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety."*

63. Relevant considerations include:

- the category of safety function(s) to be performed by the item;
- the probability that the item will be called upon to perform a safety function; and
- the potential for a failure to initiate a fault or exacerbate the consequences of an existing fault, including situations where the failure affects the performance of another safety system or component.

64. Further detail on ONR expectations can be found in TAG 94 – Categorisation of Safety Functions and Classification of Structures, Systems and Components.

65. The requirements of compliance with expectations for digital safety systems (given in TAG 31 – Safety Related Instrumentation) can be difficult to meet with a complex system of high safety significance, so Westinghouse's approach was to provide two legs to the argument:

- The system only needs to be qualified as safety-related rather than a high-class safety system; and
- Production excellence is maintained in all aspects of production from the initial specification through to the finally commissioned system and confidence-building measures to demonstrate that the system is adequate to meet the expectations for a Class 3 system.

66. I judged that this is a reasonable approach.

67. I have considered the classification based on the guidance in TAG 94. I judged that this places two requirements, for the argument that the system is Class 3 to be substantiated:

- That failure of the BEACON system cannot credibly result in operating the plant in a condition which would require the PMS to act to prevent fuel damage.
- That failure of the BEACON system (unrevealed or simultaneously with the fault) cannot degrade the function of a Class 1 protection system to the extent that a substantial increase in fuel damage is credible.

68. Westinghouse performed a failure modes and effects analysis and addressed these questions. The **AP1000** fault analysis (Ref. 14) has generally assumed that the plant limiting conditions of operation will be constrained to remain within the operating envelope defined and monitored by the BEACON system, but recognises that, in some cases, the unrevealed failure of BEACON could result in the plant operating in more adverse conditions before a fault without the operator being aware. Westinghouse assumed that Technical Specification and other limit alarms will not be silenced regardless of OPDMS functional status. It analysed selected faults – where the

conditional probability of the occurrence is sufficient to remain within the design basis (Ref. 14).

69. The consequence of the analysis was that the selected fault sequences were considered adequately protected by existing safety systems (Ref. 14). This supports the argument that the BEACON system has a limited safety impact, provided that the alternative operating limits assumed are enforced. This aspect of my assessment should be read in conjunction with the fault studies assessment of the requirements for diversity of protection to address frequent faults (Ref. 19). Based on the arguments presented relating to the consequences of BEACON system failure, I accept the argument that the proposed arrangements provide reasonable mitigation of the risk.

70. My confidence in the system has been enhanced by the results of a visit to the control-room simulator by our human factors specialist assessor (Ref. 15). The control room presents tasks ordered by critical safety functions, on a state-orientated basis. He judged that the system will help reduce the likelihood of the BEACON system leading to errors of commission.

71. He also noted that Westinghouse intends to repeat the HF ISV test, utilizing a Moorside specific AP1000 main control room simulator (per appropriate post-GDA closeout project schedules). This testing will provide data on cognitive workload and human error. WEC intends to include more simulations where instrument and interface failures occur, including presentation of credible but bad data. Specific instrument and interface failures shall be presented to the ONR during the ISV planning stages and can include failures of OPDMS information. This will help to build confidence.

72. Overall, he judged that the quality of the operator interface will help to minimise the impact of potential faults in the BEACON system.

4.2.2 ALARP Risk Reduction Measures

73. I judged that the IIS has significant advantages over the older system of movable detectors; not least that continuous monitoring of detailed core power distribution is available. I am familiar with the justification of the reactor physics model incorporated into the BEACON system (Ref. 18). I have in the past made comparisons between its output and plant data and I am therefore satisfied that the model is reasonably accurate. I did not focus on this for the current assessment. My approach was to enable Westinghouse to realise these advantages of the BEACON system while minimising potential disadvantages of its potential failure.

74. As a result of the analysis of failure modes and discussion with ONR, Westinghouse identified a number of potential safety enhancements to the design and operation of the BEACON system.

75. In the case of calibration of the ex-core detectors, Westinghouse proposed to use data from the BEACON system to calibrate the PMS and therefore determine the trip level for reactor power.

76. TAG 31 advises that the design should prevent the propagation of failures to the higher safety class systems (SAP paragraph 155). It is important to note that this SAP does not only apply to hardware failures but also to the transmission of data and digital controls. Generally, such communications should be from the higher class system to the lower class system, with the reverse prohibited by using one-way diodes or other isolation devices.

77. However, IAEA standards advise that in justified cases, signals may be sent from a lower safety class system to a higher safety class systems via individual analogue or binary signal lines, as long as the potential for failures in the lower safety class system

that could cause spurious actuation of safety classified components is assessed and is shown to be acceptable. I therefore raised this during our regular engagement (Ref. 20). Westinghouse's response was to propose to develop a software tool to simulate the response of the PMS and to provide a synthetic PMS signal in response to calibration data provided. Input of the calibration parameters into the protection system would not be permitted if the signal value fell outside the expected range. I judged that this additional measure is adequate to reduce the risk to acceptable levels.

78. I also welcomed the reinstating of surveillances and alarms to detect deviations from expected power shape, independent of the BEACON system. These signals now come from high class systems, with alarms generated by the Class 3 DDS, and BEACON provides useful additional information, which I judged will enhance safety..

79. During early interactions on this GDA issue, Westinghouse initially planned to ensure shutdown margin by relying on control rods (in addition to BEACON). However, I argued that this would leave the operators heavily reliant on BEACON surveillance 3.1.1.1 (Shutdown Margin) to protect against core damage in the event of an excess steam demand during hot zero-power operation. Normally, adequate shutdown margin (to prevent a serious reactivity transient before protection can act) is maintained by boration limits defined by the core designers, for each cycle of core operation. These limits are checked by experts in the fuel supply organisation and further checked by experts in the utility (using independent means).

80. Westinghouse agreed that retaining this good practice is a reasonably practical risk reduction (Ref. 12) and this is defined as a modification to the safety case for UK **AP1000** reactor (Ref. 13). I welcomed this change and noted that with the BEACON system operational, there is more protection available than on a conventional plant.

81. In respect of the BEACON system more generally, the SAPs advise that, where adequate reliability cannot be demonstrated, appropriate measures should be taken to ensure that the onset of failure can be detected, and that the consequences of failure are minimised. Westinghouse addressed this issue through automatic surveillance in the code system and administrative measures.

82. To ensure the integrity of the BEACON system, the performance is confirmed by pre-operational checks and several checks at different stages of the initial power ascension following refuelling. Checking of the BEACON system for operability and accuracy continues approximately every seven days, throughout the operating cycle (Ref. 11). However, these checks do not cross-compare the outputs of the redundant servers. I queried this with Westinghouse and it considered adopting additional operational checks for the UK **AP1000** reactor during maintenance (Ref. 12). The level of checking it currently proposes is limited and the arguments provided to support the proposals are weak.

83. However, I recognised that these checks are not central to ensuring the safe function of the BEACON system and the practicality of such a comparison will depend on the implementation of the BEACON hardware for UK **AP1000** reactor. I therefore noted the current proposal, but ONR will consider this further at the appropriate time. I did not consider this item of sufficient significance to merit a formal assessment finding.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

84. The BEACON system runs on an off-the-shelf commercial Linux computing server. There are two redundant servers used for core monitoring. A third is used for analysis in the technical support function. The BEACON system servers communicate with the instrumentation and the displays using the Ovation network via the DDS application servers.

85. An application implemented on the DDS provides the input data necessary and collects the BEACON system monitoring output. The intention is that the BEACON application servers will be commercial Linux servers and these will be procured at a date close to their installation. I supported this approach because, in my experience, it maximises the useful life of the system, before procurement of replacement parts becomes impractical. However, this introduces some practical difficulties in qualifying aspects of the data bus design and operating-system tools. Westinghouse produced a justification of a generic implementation of the BEACON system against the expectations of relevant standards (IEC 61513 and 62138) and this provides proof of concept.

86. Westinghouse intends to carry out a repeat of this analysis, against the requirements for systems of low safety integrity level (LowSIL) at an appropriate time during the system design. I supported this approach and drafted an assessment finding to reflect this.

87. I examined Westinghouse's analysis of its compliance to the IEC 61513 and 62138 standards (Refs 11 and 17) from the perspective of my experience of writing reactor physics codes, used for similar purposes to the BEACON system.

88. The ONR C&I inspector advised me that the structure of the Basis-of-safety Case and IEC compliance documents is in line with other **AP1000** C&I system substantiations.

89. I noted that Westinghouse has identified a number of shortfalls against the standard. These are mostly in documentation and planning of design development and in planning of testing (Ref. 11). Westinghouse made a plan to address this as the system design proceeds and I do not regard these shortfalls as an impediment at this stage. The plan will include:

- BEACON system high-level specification to identify the required application functions in a single document;
- revised performance documentation to clearly identify how performance requirements tie into performance and behaviour of the entire system;
- a formal LowSIL assessment on the delivered BEACON system;
- hardware procurement documentation consistent with UK delivery schedule;
- updated regression test documents; and
- UK-specific installation and production documents.

90. I expect module and regression testing to be used with software tools employed to identify software testing coverage. As part of the qualification of the site-specific system, Westinghouse has undertaken to provide a companion document to its regression testing specification to demonstrate that the testing set is adequately complete (Ref. 11).

91. The analysis in Ref. 11 originally dismissed certain measures which IEC 62138 did not require for LowSIL software, but which I considered reasonably practical. In particular, Westinghouse argued that there is not a requirement to employ computer-aided software engineering (CASE) tools as part of the code development and quality assurance. I judged that an element of static analysis would also be expected and some operating experience (OpEx) consideration would be appropriate. I queried the use of static analysis and Westinghouse confirmed that it does employ CASE tools, including static analysis. I am familiar with the tools the company employs and consider them suitable for the development of the modelling aspects of the BEACON

system. It is appropriate to consider the CASE tools used and the OpEx accrued again when the software for the production system is finalised.

4.4 Assessment Findings

92. During my assessment, one item was identified for a future licensee to take forward in its site-specific safety submissions:

"*The licensee shall demonstrate that the as-built design and implementation (including hardware and software elements) of the BEACON system meets the requirements of its safety function categorisation and system classification*."

93. Details of this are in Annex 1.

94. This matter does not undermine the generic safety submission and is primarily concerned with the provision of site-specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. This item is captured as an assessment finding.

95. Residual matters are recorded as assessment findings if one or more of the following apply:

- site-specific information is required to resolve this matter;
- the way to resolve this matter depends on licensee design choices;
- the matter raised is related to operator-specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters; and
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

96. The proposed assessment finding is motivated by all of these considerations.

5 CONCLUSIONS

97. This report presents the findings of the assessment of GDA Issue GI-AP1000-FD-03 relating to the **AP1000** GDA closure phase.

98. To conclude, Westinghouse presented an adequate safety case to demonstrate that reasonably practical measures were taken to ensure compliance with the fuel and fault study limits – in the event of an unrevealed failure of the BEACON code. It took measures to reduce the level to which the operators rely on the BEACON software for safety-critical activities and increased the compliance of the software lifecycle with international standards designed to ensure production excellence.

99. Further work is planned as part of the detailed design process (and this is recognised in an assessment finding) but Westinghouse has established adequate proof of concept for the use of the BEACON system in UK **AP1000** reactor.

100. I consider that from a fuel design viewpoint, this GDA issue can be closed.

6 REFERENCES

1. **AP1000** GDA Fuel Design Assessment Plan, ONR-GDA-AP-15-005, 22 April 2015, TRIM 2015/149262

2. ONR Guidance on Mechanics of Assessment, TRIM 2013/204124

3. New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-001 Revision 3, September 2016, www.onr.org.uk/new-reactors/ngn03.pdf

4. ONR How2 Business Management System. BMS: Permissioning – Purpose and Scope of Permissioning. PI/FWD – Issue 3. August 2011

5. Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. ONR. November 2014, www.onr.org.uk/saps/saps2014.pdf

6. Technical Assessment Guides:

   ONR Guidance on the Demonstration of ALARP, NS-TAST-GD-005

   Transient Analysis for DBAs in Nuclear Reactors, NS-TAST-GD-034 – Revision 2

   Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-94

   Safety of Nuclear Fuel in Power Reactors, NS-TAST-GD-075

   www.onr.org.uk/operational/tech_asst_guides/index.htm

7. Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Safety Reference Levels for Existing Reactors. WENRA. September 2014, www.wenra.org.

8. IAEA guidance:

   - Safety of Nuclear Power Plants: Design. Safety Requirements. International Atomic Energy Agency (IAEA), Safety Standards Series No. NS-R-1, IAEA, Vienna, 2000.
   - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, NS-G-1.3, IAEA, Vienna, 2002

   www.iaea.org

9. British Standards:

- Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions, BS EN 61226 2010

- Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, IEC 61513

- Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions, IEC 62138

  www.standardscentre.co.uk

10. UK AP1000 BEACON Core Monitoring System Basis of Safety Case, UKP-GW-GL-162 Revision 1, October 2016, TRIM 2016/418601

11. UK BEACON Core Monitoring System IEC 62138 Compliance Assessment, UKP-GW-GL-164 Revision 0, February 2016, TRIM 2016/68090

12. UK AP1000 BEACON Core Monitoring System ALARP Assessment, UKP-GW-GL-129 Revision 0, October 2016, TRIM 2016/394359

13. Design Change Proposal – Changes to Reduce Reliance on the Nuclear Fuels BEACON Core Monitoring System for Category B Safety Functions, APP-GW-GEE-5344 Revision 0, September 2016, TRIM 2016/394378

14. UK **AP1000** PWR Erroneous BEACON Scenario Safety Study, CN-AP1000-UK-002, 17 March 2016, TRIM 2016/119089

15. Conduct of ops. Email Steve Kerch to Richard Screeton, DCP_DCP_008536, TRIM 2016/437289

16. Chapter 19 of the "AP1000 Pre-Construction Safety Report", UKP-GW-GL-793 October 2016, TRIM 2016/142273

17. IEC 61513 Claims, Arguments and Evidence for the BEACON Core Monitoring System, UKP-GW-GL-130, TRIM 2016/316359

18. Qualification of the PHOENIX-P/ANC Nuclear Design System for Pressurised Water Reactor Cores, WCAP-11596-P-A, www.nrc.gov/docs

19. GDA Close-out for the **AP1000** Reactor GDA Issues GI-AP1000-FS-03 Diversity for Frequent Faults and GI-AP1000-FS-04 Use of In-core Detectors to Protect Against Adverse Power Distributions, ONR-NR-AR-16-024, 2016, TRIM 2016/274914

20. **AP1000** L4 Westinghouse GDA Issues Resolution – FD-03 (BEACON) – 16 June 2015, ONR-GDA-CR-15-091, TRIM 2015/232181

Annex 1

Assessment findings to be addressed during the Forward Programme – fuel design

Assessment Finding Number	Assessment Finding	Report Section Reference
GD-AP100-FD-00	Westinghouse has carried out an assessment of the adequacy of the generic BEACON system to demonstrate that a generic system meets the production excellence requirements for a Class 3 system. This has included verification of the software design against current standards and an assessment of failure modes. However, qualification of the system will need to be repeated for the site-specific design and the following finding has been raised:	Section 4.4