New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-EE-01 – PCSR Presentation of Claims, Arguments and Evidence

Assessment Report: ONR-NR-AR-16-043-AP1000
Revision 0
March 2017

Published 03/17

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

Westinghouse Electric Company (Westinghouse) 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 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 the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of electrical engineering. Specifically, this report addresses GDA Issue GI-AP1000-EE-01 Rev 0 – PCSR Presentation of Claims Arguments and Evidence

This GDA issue arose in Step 4 due to:

- The Pre-Construction Safety Report (PCSR) did not provide a clear justification of the safety case for the **AP1000** electrical distribution system. References to other sections of the PCSR did not provide any detail to relate to the overall plant safety claims.
- The PCSR did not provide a clear structure of Claims, Arguments and Evidence (CAE) which made it difficult to determine the actual safety claims due to the considerable degree of ambiguity in the PCSR.
- The electrical engineering chapter of the PCSR principally addressed the reactor with the spent fuel cooling not adequately covered.
- The description of each constituent part of the electrical system was presented as a compliance document for ONR's Safety Assessment Principles (SAP). The PCSR is required to consider the complete electrical system and substantiate the design rather than only addressing SAP compliance.

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

- Provision of a revised PCSR electrical chapter providing a clear justification of the safety case supplemented by a Basis of Safety Case (BSC) document.
- Description in the PCSR electrical chapter of the electrical support of Spent Fuel Pool (SFP) cooling consistent with the resolution of GI-AP1000-FS-01.
- Provision of a revised electrical equipment maintenance document and description in the PCSR of the minimum electrical equipment availability to support maintenance activities.
- Description in the PCSR of the role of the batteries in shutting down the plant.
- Substantiation of the electrical support for the Diverse Actuation System (DAS) consistent with the resolution of GI-AP1000-C&I-01 and GI-AP1000-C&I-02.
- Provision of a revised software verification and validation consistent with the resolution of GI-AP1000-C&I-05.
- Provision of a BSC document.

My assessment conclusions are:

- Westinghouse has presented an adequate safety case for the electrical systems of the **AP1000** reactor based on the PCSR supplemented by a structure of CAE presented in the electrical BSC.
- Westinghouse has provided an adequate UK AP1000 Plant Electrical Equipment Maintenance and Surveillance (EEMS) document which describes the approach to maintenance of the electrical equipment to support the safety of the **AP1000** reactor.

The maintainability of the plant will be demonstrated by Technical Specifications which will be finalised by the future licensee.

- Westinghouse has provided a comprehensive set of studies which demonstrate that the impacts of Grid Code operating limits have been assessed in the **AP1000** design.
- Westinghouse has provided substantiation of the electrical support for the DAS.
- Overall, I consider that the Westinghouse submissions are adequate to meet the requirements of the Resolution Plan in demonstrating the safety and integrity of the electrical distribution system.

My judgement is based upon detailed assessment of the Westinghouse safety case and supporting documents supplemented by responses to Regulatory Queries (RQ), face-to-face meetings and teleconferences.

Three 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 require licensee input/decision. These outstanding matters have been identified as Assessment Findings as follows:

- CP-AF-AP1000-EE-01: The licensee shall demonstrate that the Class 2 electrical equipment can be maintained while meeting the requirements of the Westinghouse Electrical Maintenance and Surveillance document UKP-GL-065 and the future technical requirements manual for Class 2 equipment.
- CP-AF-AP1000-EE-02: The licensee shall provide justification that all smart devices included in the Safety Class 1 Electrical Distribution System (IDS) have been validated for compliance with nuclear standards in accordance with Westinghouse Smart Device Assessment Process document UKP-GW-J0Y-004. The validation of smart devices shall be undertaken in accordance with C&I Assessment Finding CP-AF-AP1000-CI-003.
- CP-AF-AP1000-EE-03: The licensee shall substantiate during detail design of the plant the integrity of the protection relay communication links to protect against the risks of common cause failure. .

In summary I am satisfied that GDA Issue GI-AP1000-EE-01 can be closed.

LIST OF ABBREVIATIONS

AC	Alternating Current
BSC	Basis of Safety Case
C&I	Control and Instrumentation
CAE	Claims, Arguments and Evidence
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
EEMS	Plant Electrical Equipment Maintenance and Surveillance
EMI	Electro-Magnetic Interference
GDA	Generic Design Assessment
IAEA	The International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IDS	Safety Class 1 Electrical Distribution System
MWth	Megawatts (Thermal)
ONR	Office for Nuclear Regulation
PCSR	Pre-construction Safety Report
RP	Requesting Party
RQ	Regulatory Query
SAP	Safety Assessment Principle
SFP	Spent Fuel Pool
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
UPS	Uninterruptible Power Supply
US NRC	United States (of America) Nuclear Regulatory Commission

TABLE OF CONTENTS

Table(s)

Annex

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company LLC (Westinghouse) is the reactor design company for the **AP1000®** reactor. Westinghouse completed GDA Step 4 (Ref.1) 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 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.

2. This report is the Office of Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of electrical engineering. Specifically, this report addresses GDA Issue GI-AP1000-EE-01 – Presentation of PCSR Claims, Arguments and Evidence.

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

1.2 Scope

4. The scope of this assessment is detailed in assessment plan ONR-GDA-AP-14-006.

5. The scope of assessment focused on determining whether Westinghouse has produced a safety case which substantiates the design of the complete plant electrical distribution system. This was required to be in a structure of Claims, Arguments and Evidence (CAE) to demonstrate that the electrical system meets the requirements of its safety role as specified in the other chapters of the Pre-Construction Safety Report (PCSR).

6. The work focussed on establishing safety claims on the electrical distribution system to support plant safety systems. I assessed the safety case to establish that it provides a clear structure of electrical system claims based on providing support to safety claims covering plant safety systems. I then assessed whether appropriate arguments and evidence were provided to substantiate the claims.

7. I assessed further claims regarding the resilience of the electrical system to common cause failures from threats posed by electrical system disturbances, internal and external hazards and software errors. I used the same assessment approach as for the claims covering support to plant safety systems by determining whether adequate arguments and evidence had been provided to support the claims.

8. Westinghouse proposed in the Resolution Plan, a structured presentation of the safety features in the AP1000 reactor design which supported resolution and progressing of concerns from earlier steps such as maintenance philosophy, Grid Code compliance and equipment availability. The structured presentation of the safety case resolved a number of concerns and also enabled identification and resolution of additional issues. This report addresses the resolution of these additional issues.

9. The scope of assessment is appropriate as it focusses on assessment of the safety case for the electrical system in accordance with the GDA Step 4 scope.

1.3 Method

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

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

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

12. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (http://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 CAE to substantiate the adequacy of the AP1000 design reference point.

13. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, to provide the claims, arguments and evidence to substantiate the adequacy of AP1000 reactor design reference point.

14. This report considers the adequacy of the PCSR and supporting Basis of Safety Case (BSC) to substantiate the adequacy of the electrical distribution system to support the plant safety systems

2.2 Standards and criteria

15. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) (Ref. 3), internal TAGs (Ref. 4), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites.

2.3 Safety Assessment Principles

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

2.4 Technical Assessment Guides

17. The following TAG has been used as part of this assessment:

- Essential Services: NS-TAST-GD-019

2.5 National and International Standards and Guidance

18. The following international standards and guidance have been used as part of this assessment (Refs. 5 to 6):

- IAEA Standard SSG34: Design of Electrical Power Systems for Nuclear Power Plants
- IAEA Standard SSR-2/1: Safety of nuclear power plants: Design

2.6 Use of Technical Support Contractors (TSCs)

19. No Technical Support Contractors have been used during this assessment.

2.7 Integration with Other Assessment Topics

20. 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.

21. I have assessed the requirements for electrical power supplies to support the Spent Fuel Pool (SFP) cooling in conjunction with fault studies assessors by assessing the Westinghouse CAE submissions and referencing to the fault studies safety case. In support of this assessment I have held meetings and teleconferences with the electrical and fault studies teams of the Requesting Party (RP) and ONR fault studies assessors to clarify safety claims and supporting documentation.

22. In assessing the claims regarding Grid Code compliance I have consulted with fault studies assessors to advise on the limits for frequency variations established within the Grid Code so that implications for reactor operation could be assessed within the fault studies discipline.

23. I have co-ordinated with Control and Instrumentation (C&I) assessors to ensure consistency of the power supply provisions for the diverse actuation with C&I requirements for diversity and redundancy of supplies.

24. I have assessed the Westinghouse claims regarding the use of smart devices on electrical systems in conjunction with C&I assessors. This has enabled a consistent approach to be adopted in the assessment of the use of smart devices in C&I systems and the power supplies to these systems.

25. I have supported the integration with the other assessment topics by raising a number of Regulatory Queries (RQ) (Ref. 9). These RQs have requested supporting technical information and supporting references to assess the consistency of the safety case across the technical disciplines. The responses to the RQs have informed my overall assessment of the Westinghouse safety case.

2.8 Out of scope items

26. The requirement of the GDA Issue was to produce a PCSR with claims, arguments and evidence to substantiate the **AP1000** reactor design assessed in GDA Step 4. Consequently, the out of scope items remain unchanged from GDA Step 4. The following out of scope items were identified in GDA Step 4:

- detailed design and specification of main items
- detailed fast transient assessment
- grid connection arrangements
- detailed site-specific study of the electrical system including load flows, fault studies, transient performance etc.
- site-specific protection co-ordination study

3 REQUESTING PARTY'S SAFETY CASE

27. The Westinghouse safety case for GDA Issue GI-AP1000-EE-01 is described in the following documents:

- UKP-GW-GL-163 Rev. 2 – UK AP1000 Electrical Basis of Safety Case
- UKP-GW-GL-793 Rev. 1 – UK AP1000 Pre Construction Safety Report Chapter 18
- UKP-GW-GL-065 Rev. 5 – UK AP1000 Plant Electrical Equipment Maintenance and Surveillance
- UKP-GW-GLR-031 Rev. 0 – AP1000 UK Grid Code Compliance Report

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-EE-01

28. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 7).

4.1 Scope of Assessment Undertaken

29. The scope of the assessment has been to consider the expectations detailed in the GDA Issue, GI-AP1000-EE-01(Ref. 8) and the associated GDA Issue action. These are detailed within Annex 3 of this report.

30. The assessment has considered whether the submissions provide the CAE to substantiate the design of the complete plant electrical distribution system which are related to the overall safety claims of the plant.

31. Where further supporting documents to support the assessment have been required I have raised RQs (Ref. 9). The Westinghouse responses to these RQs have helped to inform my assessment of the **AP1000** reactor electrical system design.

4.2 Assessment

4.2.1 PCSR

32. GDA Issue GI-AP1000-EE-01 requires the PCSR to incorporate a structure of CAE to demonstrate that the electrical system fully meets the requirements of its safety role as defined in the other chapters of the PCSR. The GDA Issue presented the following ONR expectations for the PCSR:

- The PCSR should provide a clear justification of the safety case for the **AP1000** electrical system. References to other sections of the PCSR should provide detail to relate to the overall plant safety claims.
- There should be a clear structure of CAE to avoid any ambiguity in the safety claims.
- Chapter 18 of the PCSR (Ref. 10) which covers electrical engineering should cover the safety claims associated with the SFP in addition to the claims on the reactor and its supporting systems.
- The PCSR should consider the safety case for the complete electrical system rather than an assessment of constituent parts. This assessment should not be presented as a compliance document for ONR’s SAPs.

33. Westinghouse has responded to the GDA Issue by presenting the safety claims in a BSC (Ref. 11) document which supports the PCSR. The ONR assessment of the BSC is addressed in Section 4.2.2.

34. Westinghouse has updated Chapter 18 of the PCSR to describe the features of the **AP1000** reactor electrical system which support the plant safety systems, with detailed safety claims presented in the BSC document.

35. Chapter 18 of the PCSR describes the design principles to be applied to the electrical systems and provides a description of the electrical architecture. This includes a description of the Class 2 Alternating Current (AC) distribution system together with the standby diesel generators and ancillary diesel generators. Chapter 18 describes the design features of the Class 1 and Class 2 battery-powered systems to substantiate their role in supporting plant safety systems.

36. Chapter 18 describes external interfaces which cover SFP cooling, provisions to enhance resilience in response to the ONR report Japanese earthquake and tsunami: Implications for the UK nuclear industry (Ref. 12) and post-accident monitoring provisions.

37. The approach to the use of smart devices on the electrical system is presented by describing the process for validation and verification of embedded software in electrical systems. The provisions to protect against the effects of common cause failure due to software failures are described.

38. I consider that the PCSR Chapter 18 presents an adequate description of the safety provisions on the electrical systems of the **AP1000** reactor. Assessment Findings as detailed in Section 4.4 will be raised covering validation of smart devices and provision of technical specifications which define standby diesel availability requirements. I consider with the commitment for future resolution of the Assessment Findings that PCSR Chapter 18 of the PCSR is sufficient to support close-out of the GDA Issue.

4.2.2 Basis of Safety Case

39. The BSC supports the electrical safety case in Chapter 18 of the PCSR. The electrical BSC presents the plant electrical safety claims and associated arguments and evidence. The claims have been presented in a structure of 11 high-level claims which are supported by more detailed lower-level sub-claims.

40. The safety claims in the BSC have been related to claims regarding the provision of electrical power to support the requirements of plant safety systems. Other chapters of the PCSR provide clear references to the claims on the electrical system. The BSC provides supporting arguments and evidence to substantiate the claims.

41. The BSC makes claims regarding the resilience of the electrical system to sources of common cause failure which could potentially impact on multiple divisions of the electrical distribution system. It provides appropriate evidence to support the claims based on Westinghouse design documentation. In some instances detailed evidence is not yet available or evidence related to the **AP1000** reactor design will need to be developed. In these instances, reference is made to the provision of a future document which will provide the appropriate evidence as part of detailed design.

42. I have assessed the structure of the PCSR and supplementary BSC document that presents the safety case for the **AP1000** reactor electrical system. I consider that the CAE based structure provides a sound basis for demonstrating the safety case for the **AP1000** reactor electrical system.

43. I have assessed the safety claims submitted in the BSC document against the requirements of ONR's SAPs and consider that the claims adequately demonstrate the safety role of the electrical system for the **AP1000** reactor.

44. I have assessed the arguments and evidence presented in support of the safety claims which are based on generic design documentation. This is supplemented by commitments to provide design documentation as future evidence where the evidence will become available during the detailed design process. I consider that this presentation adequately presents the justification of the safety role of the electrical system on the **AP1000** reactor.

45. My overall assessment of the BSC is that it provides an adequate presentation of the safety case for the **AP1000** reactor electrical system in a CAE structure as required by GDA Issue GI-AP1000-EE-01.

4.2.3 UK AP1000 Plant Electrical Equipment Maintenance and Surveillance

46. The resolution plan for GDA Issue GI-AP1000-EE-01 identifies a deliverable to demonstrate that the electrical equipment can be adequately maintained and remain compliant with the safety case requirements. Westinghouse has addressed this by updating the document UK AP1000 Plant Electrical Equipment Maintenance and Surveillance (EEMS) (Ref. 13). This document describes the overall philosophy of the maintenance requirements for the **AP1000** reactor electrical distribution system components which support Category A and Category B safety functions. The electrical BSC provides claims and supporting arguments and evidence related to the electrical plant maintenance requirements.

47. I have assessed these submissions and consider that they provide overall high-level requirements for undertaking maintenance of the electrical equipment to support the safety case. This assessment has been informed by responses to RQs raised by ONR. I consider that the approach described for performing periodic maintenance operations in the EEMS document is acceptable to support safe operation of the plant.

48. I have assessed the supporting arguments and evidence to support the claim on maintainability of the Class 1 systems based on the equipment availability requirements defined by the Class 1 Operational Technical Specifications (Ref.14). I consider that this describes adequate provisions for conducting maintenance of plant items whilst ensuring equipment availability to support safe operation of the plant.

49. Westinghouse has submitted the document Recommendation for development of the AP1000 Technical Requirements Manual (Ref.25). This document states that the technical requirements manual when developed will include Operational Technical Specifications to define availability requirements for Class 2 equipment. I consider that this future approach presents an acceptable process for demonstrating the maintainability of the Class 2 electrical equipment. However, as the Operational Technical Specifications for Class 2 equipment are not available I do not consider that Westinghouse has fully demonstrated that the Class 2 equipment can be accessed to provide adequate maintenance in line with the defined requirements.

50. In conclusion I consider that the maintainability of the Class 1 equipment has been adequately demonstrated by the submissions. I do not consider that the maintainability of the Class 2 systems has been adequately substantiated due to the non-availability of the Operational Technical Specifications. The requirement to produce the Operational Technical Specifications covering all electrical equipment is covered by existing Assessment Finding AF-AP1000-EE-31 which was raised in the Step 4 assessment report

51. In order to establish the maintainability of electrical equipment based on operational Technical Specifications I have raised an additional Assessment Finding CP- AF-AP1000-EE-01 which requires the future licensee to demonstrate that the Class 2 electrical equipment can be maintained while meeting the requirements of the EEMS document and technical requirements manual for Class 2 equipment.

4.3 Technical Issues Arising from Assessment

52. The presentation of the safety case in a CAE format in the electrical BSC has resulted in identification of a number of technical issues which have required resolution as part of the close-out of the GDA Issue.

53. Westinghouse has addressed the resolution of these issues either by the submission of appropriate documentation or by demonstrating an acceptable methodology which will be used to resolve the issue. The implementation of these methodologies is the subject of Assessment Findings for final resolution by the future licensee during the detail design phase.

54. My assessment of the resolution of the individual issues is presented in the following sections.

4.3.1 Grid Code Compliance

55. I examined the arguments and evidence supporting the high-level safety claim in the electrical BSC regarding compliance with the Grid Code (Ref. 16). The claim is that the **AP1000** reactor electrical system will safely remain connected to the grid through all disturbances defined in the Grid Code. The argument supporting this claim is that the **AP1000** reactor will reliably deliver power to the grid under all required frequency and voltage conditions; without violating the safety requirements of the plant or any of its support systems.

56. This reflects a requirement for compliance with the Grid Code that generating plant should remain connected to the grid through defined disturbances in order to support a stable grid system and security of supplies.

57. Final agreement for connection of the **AP1000** reactor to the grid system will be part of the licensing process, taking account of the results of studies based on detailed design data. The objective of the Grid Code compliance document is to support the BSC by demonstrating the safety of the plant when the electrical system is subjected to the disturbances defined by the Grid Code.

58. Westinghouse has provided supporting evidence for the arguments covering Grid Code compliance by preparing document AP1000 UK Grid Code Compliance Report (Ref. 17). This has identified 53 relevant Grid Code clauses and has confirmed full compliance with 37 of these clauses.

59. Westinghouse has identified a high probability of compliance for the remaining 16 clauses. This is supported by detailed studies carried out to demonstrate suitability of the design based on generic design information. Full compliance with the Grid Code will be demonstrated with final site-specific design data; I consider that the use of generic data at this stage is adequate for GDA purposes.

60. The 16 clauses identified as having a high probability of compliance cover fault ride through, minimum frequency response and operating range, operating modes including Frequency Sensitive Mode and Limited Frequency Sensitive Mode and plant performance requirements. The key clauses relate to:

- grid frequency variations
- compliance with fault ride through capability, including short circuit and super grid voltage dips
- operation in Frequency Sensitive Mode
- operation in Limited Frequency Sensitive Mode.

61. ONR fault studies has assessed the grid frequency variations clause as part of close-out of GDA Issue GI-AP1000-FS-03 (Ref. 19). The ONR fault studies close-

out report states that ONR is satisfied that Westinghouse has presented a case that adequately demonstrates that the **AP1000** reactor can remain safely connected to the grid throughout the range of operating frequencies defined within the Grid Code.

62. I have sampled the evidence supporting the compliance claims for the above Grid Code clauses. I consider that the studies are adequate in demonstrating the capability of the plant to operate safely when subject to the disturbances defined in the Grid Code.

63. My assessment of the compliance report and supporting documents is that they demonstrate adequate capability of the **AP1000** reactor to generate safely when subject to the disturbances defined in the Grid Code. The studies need to be finalised during detailed design to take into account site-specific data, Assessment Finding AF-AP1000-EE-011 requiring the future licensee to confirm Grid Code compliance for each power plant was raised during the Step 4 assessment.

64. I am satisfied that the evidence provided by Westinghouse supports the claim that there is a high probability that the **AP1000** reactor will achieve compliance with the Grid Code during the site licensing phase when further detailed design data becomes available.

4.3.2 Smart devices used in the electrical system

65. Westinghouse has made claims in the electrical BSC regarding the approach to be adopted for the use of smart programmable devices on the plant electrical distribution system. These claims are made to define the role of the electrical distribution system in meeting the guidance in Chapter 5 of the PCSR (Ref. 10) that digital devices used in the Safety Class 1 Electrical Distribution System (IDS) system will be assessed for compliance with Class 1 nuclear standards.

66. The potential use of smart devices has been identified in a number of applications on the Class 1 IDS system including inverters, static switches and digital trip breakers. Westinghouse has identified in the electrical BSC that these will be specified to nuclear standards and assessed for compliance with these standards. The electrical BSC states that if compliance with nuclear standards is not achievable that alternative equipment will be utilised which does not use smart components.

67. Westinghouse has addressed the potential for common cause failure between the inverter and static switch on the IDS supply by confirming that, where smart devices are used, the software on the inverter will be from a different source to that on the static switch.

68. I have assessed the Westinghouse claims through discussions in meetings with Westinghouse, when I have requested a number of clarifications and have requested further information to support the claims by raising RQs. The responses to these RQs have informed my assessment. Based on my assessment as supported by the RQ responses I consider that the approach described in the BSC is acceptable.

69. The implementation of procedures to correctly specify requirements and to carry out assessments and justifications is the responsibility of the future licensee during detailed design. I have, therefore, raised Assessment Finding CP-AF-AP1000-EE-02 which requires the licensee to provide justification that all smart devices included in the Class 1 IDS system have been validated for compliance with nuclear or equivalent standards as outlined in United Kingdom AP1000 Smart Device Assessment Process document UKP-GW-J0Y-004 (Ref.27).

4.3.3 Networking of Electrical Protection Relays

70. Westinghouse describes in the electrical BSC the networking arrangements for communication between the protection relays and the plant control system. For Class 1 systems this is claimed as utilising a read-only data link which is intended to prevent the transfer of information from the data concentrator to the Class 1 protection relays. Additionally, this link will be used only for status monitoring from the relays. Evidence to support this is provided in the **AP1000** Plant Control System and Data Display and Processing System Interface Specification (Ref. 20).

71. I have sought clarification of the claims by raising RQs (Ref. 9) and based on these responses I am content that the specified requirements address potential issues of common cause failure arising from propagation of faults from the DDS through the data concentrator. However, the details of these provisions will need to be determined during detail design and I have raised Assessment Finding CP-AF-AP1000-EE-03 which requires the future licensee to substantiate the integrity of the protection relay communication links to protect against the risks of common cause failure.

72. Westinghouse describes the networking arrangements provided for monitoring and control from Class 2 and Class 3 protection relays. These arrangements provide for status monitoring from the protection relays and for control of circuit breaker switching through these relays using hard-wired connections from the PLS. I consider that Westinghouse has provided appropriate evidence to demonstrate that the control link is hardwired with no potential for common cause failure due to software links. The status monitoring is via the one-way link used for Class 1 relays described above.

73. Based on the evidence provided I am content that Westinghouse has demonstrated that it has made adequate provisions to address the risk of common cause failure due to software issues. In conclusion, I am satisfied that Westinghouse has provided adequate evidence to substantiate the safety claims in this area.

4.3.4 Spent Fuel Cooling

74. I have assessed the provision of electrical power supplies to support SFP cooling operations. This assessment takes account of the close-out of GDA Issue GI-AP1000-FS-01 (Ref. 21) covering the SFP safety case.

75. Westinghouse has identified the claims on the provision of electrical power supplies to support the cooling requirements as defined in the SFS Component Control Requirements (Ref. 22). The electrical BSC references the claim on electrical supplies and provides appropriate arguments and evidence to support the claim on the provision of power supplies to support SFP cooling.

76. Availability requirements are defined for the provision of power supplies from the standby diesel generators. These define a higher availability requirement for the standby diesel generators when the decay heat in the fuel pool is greater than or equal to 4.0 Megawatts (Thermal) (MWth). The capability of the standby diesel generators to meet this requirement cannot be fully assessed until the Operational Technical Specifications for Class 2 equipment are completed. Assessment Finding AF-AP1000-EE-31**,** which was raised in the Step 4 report, requires the future licensee to produce these Technical Specifications.

77. I conclude that Westinghouse has presented a case for GDA purposes to demonstrate that the power supply provisions adequately support the cooling of

the SFP. This is based on demonstration in the BSC of main and standby sources of power to support the claims on the electrical system identified in the fault studies discipline. During detail design this will need to be supported by the response to Assessment Finding AF-AP1000-EE-31 to demonstrate the maintainability of electrical equipment while supporting adequate availability to meet the safety case requirements.

4.3.5 Availability Requirements for Electrical Equipment

78. GDA Issue GI-AP1000-EE-01 identified a requirement to demonstrate the ability to take electrical equipment out of service to carry out maintenance required to support continuing reliable operation. Westinghouse states in Claim 6 that appropriate provisions are made for periodic inspection to be implemented in accordance with the Operational Technical Specifications to ensure reliability and availability of the equipment.

79. The evidence provided in the BSC and maintenance and surveillance document adequately addresses the requirements to perform regular and systematic maintenance on the electrical equipment and describes the high-level principles to be adopted in performing this work. I consider this to be adequate for GDA purposes.

80. The Operational Technical Specifications that describe the availability requirements for Class 1 equipment provide adequate demonstration of these requirements.

81. I do not consider that Westinghouse has provided full demonstration of the ability of the Class 2 electrical equipment to be taken out of service for maintenance purposes. This is due to the Technical Requirements Manual covering Class 2 equipment being a statement of intent and not providing detailed Operational Technical Specification availability requirements.

82. I consider that the maintainability will need to be demonstrated as part of detail design. Section 4.2.3 refers to Assessment Finding CP-AF-AP1000-EE-01 which requires the future licensee to demonstrate that the Class 2 equipment can be maintained while meeting the requirements of the EEMS document and Technical Requirements Manual for Class 2 equipment.

83. I conclude that Westinghouse has defined an adequate structure for demonstrating the availability of electrical equipment to support safety systems. This can only be completed once the availability requirements for electrical equipment are defined.

4.3.6 Power Supplies to Diverse Actuation System (DAS)

84. In conjunction with the ONR C&I team, I have assessed the arrangements of the power supplies to the DAS in the Basis of Safety Case for the Diverse Actuation System (DAS BSC) (Ref. 23) and the electrical BSC. This assessment forms as part of the close-out of GDA Issue GI-AP1000-CI-02: DAS – Adequacy of Architecture (Reference 24), Action A3 which was referenced in the Electrical Step 4 report.

85. Action A3 required Westinghouse to update the **AP1000** reactor BSC for the DAS so that it identifies and provides a description of the sources of electrical power for the DAS and their physical location on the plant.

86. Westinghouse has updated the DAS BSC in response to the GDA Issue so that it clearly addresses the issues raised in Action A3, including stating the location and

sources of supply (including the Safety Class and Division) and the Safety Class, location and capacity of the dedicated DAS batteries and any other sources of power required for the DAS to operate. The DAS BSC includes arguments and evidence to substantiate the claims regarding the adequacy of the electrical supplies.

87. I have assessed the Westinghouse response to Action A3, including the relevant parts of the DAS BSC and electrical BSC. I am satisfied with the Westinghouse response to Action A3. I consider the DAS BSC now adequately addresses the issues raised and provides a clear description of the sources of electric power for the DAS and their physical location on the plant. I consider that the electrical BSC adequately demonstrates the diversity and redundancy of power supplies to the DAS.

88. The detailed specifications for the Uninterruptible Power Supply (UPS) units are not identified. These specifications should show that the UPS is appropriate for its safety-related duty. Assessment Finding AF-AP1000-EE-018 was raised during the Step 4 assessment to cover this work and requires the future licensee to prepare detailed specifications for electrical equipment.

89. I conclude that the Westinghouse submission satisfactorily addresses GDA Issue GI-AP1000-CI-02, Action 3 by describing adequate arrangements for power supplies to the DAS.

4.3.7 Protection from Electromagnetic Interference on Squib Valve Supplies

90. I have assessed the evidence supporting the Westinghouse claims regarding protection from Electromagnetic Interference (EMI) which are presented in the electrical BSC. In particular, in conjunction with the mechanical assessor, I have assessed the supporting evidence for protection in the electrical system from EMI causing spurious operation of the squib valves which are required to support the Squib valve concept and design substantiation (Ref.15) document. Assessment of the effects of EMI on the squib valve pyrotechnics is covered in the close-out report of GDA Issue GI-AP1000-ME-01: Squib valve concept and design substantiation (Ref. 26).

91. I consider that the arguments and evidence provided in the electrical BSC and Chapter 18 of the PCSR demonstrate appropriate provisions in the design of the plant electrical systems to protect from the effects of EMI on the plant. Consequently, I am content that the evidence provided adequately supports the claims and arguments. In addition, Westinghouse has adequately addressed in the supporting evidence the particular claims associated with the squib valves.

92. In conclusion, I consider that Westinghouse has demonstrated that the **AP1000** reactor electrical system design provides appropriate protection from EMI impacting on the operation of the squib valves.

4.4 Assessment Findings

93. During my assessment, I identified three items for a future licensee to take forward to its site-specific safety submissions. Details of these are contained in Annex 1.

94. These matters do not undermine the generic safety submission and are 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. These items are captured as Assessment Findings.

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;
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

96. Each of the identified Assessment Findings meets a number of these criteria.

5 CONCLUSIONS

97. This report presents the findings of the assessment of GDA Issue GI-AP1000-EE-01 relating to the **AP1000** reactor GDA closure phase.

98. The conclusions of my assessment are as follows:

- Westinghouse has presented an adequate safety case for the electrical systems of the **AP1000** reactor based on the PCSR supplemented by a structure of CAE presented in the electrical BSC. I have assessed the Westinghouse submissions for compliance with the requirements of the ONR SAPs defined in Table 1 and consider that the requirements are fully satisfied.

- Westinghouse has provided an adequate EEMS document which describes the approach to maintenance of the electrical equipment to support the safety of the **AP1000** reactor. The maintainability of the plant will be demonstrated by Technical Specifications which will be finalised by the future licensee.

- Westinghouse has provided a comprehensive set of studies which demonstrate that the impacts of Grid Code operating limits have been assessed in the **AP1000** reactor design.

- Westinghouse has provided substantiation of the electrical support for the DAS.

- Overall, I consider that the Westinghouse submissions are adequate to meet the requirements of the Resolution Plan in demonstrating the safety and integrity of the electrical distribution system.

99 My assessment has identified the following Assessment Findings for the future licensee to address during detail design and incorporate in site-specific safety submissions:

- CP-AF-AP1000-EE-01: The licensee shall demonstrate that the Class 2 electrical equipment can be maintained whilst meeting the requirements of the Westinghouse EEMS document UKP-GL-065 and the future technical requirements manual for Class 2 equipment.

- CP-AF-AP1000-EE-02: The licensee shall provide justification that all smart devices included in the Safety Class 1 IDS have been validated for compliance with nuclear standards in accordance with Westinghouse Smart Device Assessment Process document UKP-GW-J0Y-004. The validation of smart devices shall be undertaken in accordance with C&I Assessment Finding CP-AF-AP1000-CI-003.

- CP-AF-AP1000-EE-03: The licensee shall substantiate during detail design of the plant the integrity of the protection relay communication links to protect from the risks of common cause failure.

100. On the basis of the above conclusions, I consider that from an electrical engineering view point, the **AP1000** reactor design is suitable for construction in the UK.

6 REFERENCES

1	Step 4 Electrical Systems Assessment of the Westinghouse AP1000® Reactor. ONR Assessment Report ONR-GDA-AR-11-007 Revision 0. November 2011. TRIM Ref. 2010/581524
2	Guidance on Mechanics of Assessment within the Office for Nuclear Regulation (ONR).ONR. TRIM Ref. 2013/204124
3	Safety Assessment Principles for Nuclear Facilities. Revision 0. ONR. November 2014. http://www.onr.org.uk/saps/saps2014.pdf
4	Technical Assessment Guides. ONR. http://www.onr.org.uk/operational/tech_asst_guides/index.htm
5	Design of Electrical Power Systems for Nuclear Power Plants. International Atomic Energy Agency (IAEA). Safety Standards Series No. SSG34. IAEA. Vienna. 2016. http://www-pub.iaea.org/books/IAEABooks/10688/Design-of-Electrical-Power-Systems-for-Nuclear-Power-Plants
6	Safety of nuclear power plants: Design. International Atomic Energy Agency (IAEA). Safety Standards Series no. SSR-2/1 (rev. 1). IAEA. Vienna. 2016. http://www-pub.iaea.org/books/iaeabooks/10885/Safety-of-Nuclear-Power-Plants-Design
7	Purpose and Scope of Permissioning. ONR Guide. August 2015. TRIM Ref. 2015/304735
8	PCSR Presentation Of Claims Arguments And Evidence**.** GDA Issue GI-AP1000-EE-01 Revision 0. TRIM Ref. 2011/369316
9	RQ-AP1000-1347: Draft of claims arguments and evidence for the electrical system - Full response. TRIM Ref. 2015/322797 RQ-AP1000-1377: Compliance with UK Grid Code – Full response. TRIM Ref.2015/367318 RQ-AP1000-1404: WEC response on Grid Code compliance – Full Response. TRIM Ref.2015/431040 RQ-AP1000-1412: Basis of Safety Case September 2015 – Full Response. TRIM Ref.2015/447596 RQ-AP1000-1432: Electrical equipment maintenance and surveillance – Full Response. TRIM Ref.2016/181319. RQ-AP1000-1500: PCSR Chapter 18 – Full Response. TRIM Ref.2016/181377 RQ-AP1000-1534: AP1000 Grid Code compliance assessment – Full Response. TRIM Ref.2016/196675 RQ-AP1000-1544: AP1000 Basis of Safety Case - Full Response. TRIM

	Ref.2016/223727 RQ-AP1000-1666: Basis of Safety Case evidence structure – Full Response. TRIM Ref. 2016/348770 RQ-AP1000-1708: Queries on AP1000 Electrical BSC - Full Response. TRIM Ref. 2016/412913
10	**AP1000** Pre-Construction Safety Report. UKP-GW-GL-793 Revision 1, January 2017. TRIM Ref.2017/43700
11	UK **AP1000®** Electrical Basis of Safety Case. UKP-GW-GL-163 Revision 2. Westinghouse. December 2016. TRIM Ref. 2016/495021
12	Japanese earthquake and tsunami: Implications for the UK nuclear industry. ONR Report ONR-FR-REP-11-002 Revision 2. September 2011. http://www.onr.org.uk/fukushima/final-report.pdf
13	UK **AP1000®** Plant Electrical Equipment Maintenance and Surveillance. UKP-GW-GL-065 Revision 5. Westinghouse. July 2016. TRIM Ref. 2016/285512
14	UK **AP1000®**Technical Specifications. UKP-GW-GL-501 Revision 0. Westinghouse. January 2016. TRIM Ref. 2016/40641
15	**AP1000** Squib Valve Safety Case. UKP-GW-GL-200 Revision 1. Westinghouse. December 2016.TRIM Ref. 2016/475177
16	The Grid Code. Issue 5 Revision 19. National Grid Electricity Transmission PLC. September 2016
17	**AP1000** UK Grid Code Compliance Report. UKP-GW-GLR-031 Revision 0. Westinghouse. July 2016. TRIM Ref. 2016/265464
18	Diversity for Frequent Faults, GDA Issue GI-AP1000-FS-03 Revision 0. TRIM Ref. 2011/369327
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 Rev 0. TRIM Ref. 2016/274914
20	**AP1000** Plant Control System and Data Display and Processing System Interface Specification. APP-GW-J4-079 Revision 1. Westinghouse. November 2015. TRIM Ref. 2016/363674
21	Spent Fuel Pool Safety Case. GDA Issue GI-AP1000-FS-01 Revision 0. TRIM Ref. 2011/369323
22	SFS component control requirements. APP-SFS-M3C-100 Revision 8.

	Westinghouse. November 2013 TRIM Ref. 2017/24585
23	UK **AP1000** Basis of Safety Case for the Diverse Actuation System. UKP-DAS-GLR-001 Revision 2 Westinghouse. December 2016. TRIM Ref. 2016/296907
24	DAS – Adequacy of Architecture. GDA Issue GI-AP1000-CI-02 Revision 0. TRIM Ref. 2011/369297
25	Recommendation for development of the **AP1000** Technical Requirements Manual. UKP-GW-GL-502 Revision 0. Westinghouse. February 2016. TRIM Ref. 2016/54147
26	GDA Issue GI-AP1000-ME-01: Squib valve concept and design substantiation. TRIM Ref. 2016/275007
27	United Kingdom AP1000 Smart Device Assessment Process. UKP-J0Y-004 Rev. 2. Westinghouse. December 2016. TRIM Ref. 2016/497351

Table 1

Safety Assessment Principles Considered for Close-out of GI-AP1000-EE-01 Rev 0

SAP No	SAP Title	Description
EQU.1	Qualification Procedures	Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.
EDR.1	Failure to safety	Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.
EDR.2	Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.
EDR.3	Common cause failure	Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.
EDR.4	Single failure criterion	During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.
ERL.2	Measures to achieve reliability	The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.
ERL.4	Margins of conservatism	Where multiple safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a margin of conservatism with allowance for uncertainties.
EMT.1	Identification of requirements	Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.
EMT.3	Type-testing	Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.

Table 1

Safety Assessment Principles Considered for Close-out of GI-AP1000-EE-01 Rev 0

SAP No	SAP Title	Description
EMT.6	Reliability claims	Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals throughout plant life commensurate with the reliability required of each item.
EMT.7	Functional testing	In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.
ELO.1	Access	The design and layout should facilitate access for necessary activities and minimise adverse interactions during such activities.
EHA.10	Electromagnetic interference	The design of facility should include protective measures against the effects of electromagnetic interference.
ESS.1	Requirement for safety systems	All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.
ESS.2	Determination of safety system requirements	The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.
ESS.3	Monitoring of plant safety	Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.
ESS.7	Diversity in the detection of fault sequences	The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.
ESS.8	Automatic initiation	A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.
ESS.9	Time for Human Intervention	Where human intervention is necessary following the start of a requirement for protective action, then the time before such intervention is required should be demonstrated to be sufficient.
ESS.10	Definition of capability	The capability of a safety system, and of each of its constituent sub-systems and components, should be defined.
ESS.11	Demonstration of adequacy	The adequacy of the system design as the means of achieving the specified function and reliability should be demonstrated for each system.

SAP No	SAP Title	Description
ESS.12	Prevention of service infringement	Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components.
ESS.15	Alteration of configuration, operational logic or associated data	No means should be provided, or be readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels etc.) may be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.
ESS.16	No dependency on external sources of energy	Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.
ESS.19	Dedication to a single task	A safety system should be dedicated to the single task of performing its safety function.
ESS.20	Avoidance of connections to other systems	Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided
ESS.21	Reliability	The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.
ESS.23	Allowance for unavailability of equipment	In determining the safety system provisions, allowance should be made for the unavailability of equipment.
ESS.24	Minimum operational equipment requirements	The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.
EES.1	Provision	Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and fault conditions.
EES.2	Sources external to the site	Where a service is obtained from a source external to the nuclear site, that service should also be obtainable from a back-up source on the site.
EES.3	Capacity, duration, availability and reliability	Each back-up source should have the capacity, duration, availability and reliability to meet the maximum requirements of its dependent systems.
EES.4	Sharing with other plants	Where essential services are shared with other plants on a multi-facility site, the effect of the sharing should be taken into account in assessing the adequacy of the supply.
EES.5	Cross-connections to other services	The capacity of the essential services to meet the demands of the supported safety functional requirement(s) should not be undermined by making cross-connections to services provided for non-safety functions.
EES.6	Alternative sources	Alternative sources of essential services should be designed so that their reliability would not be prejudiced by adverse conditions in the services to which they provide a back-up

SAP No	SAP Title	Description
EES.7	Protection devices	Protection devices provided for essential service components or systems should be limited to those that are necessary and that are consistent with facility requirements.
EES.8	Sources external to the site	Where a source external to the nuclear site is employed as the only source of the essential services needed to provide adequate protection, the specification and in particular the availability and reliability should be the same as for an on-site source.
EES.9	Loss of service	Essential services should be designed so that the simultaneous loss of both normal and back-up services will not lead to unacceptable consequences.
EKP.3	Defence in Depth	A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.
EKP.5	Safety measures	Safety measures should be identified to deliver the required safety function(s).

Annex 1

Assessment Findings to be addressed during the Forward Programme – Electrical Engineering

Assessment Finding Number	Assessment Finding	Report Section Reference
CP-AF-AP1000-EE-01	The licensee shall demonstrate that the Class 2 electrical equipment can be maintained whilst meeting the requirements of the Westinghouse EEMS document UKP-GL-065 and the future technical requirements manual for Class 2 equipment.	4.2.3
CP-AF-AP1000-EE-02	The licensee shall provide justification that all smart devices included in the Safety Class 1 IDS have been validated for compliance with nuclear standards in accordance with Westinghouse Smart Device Assessment Process document UKP-GW-J0Y-004. The validation of smart devices shall be undertaken in accordance with C&I Assessment Finding CP-AF-AP1000-CI-003.	4.3.2
CP-AF-AP1000-EE-03	The licensee shall substantiate during detail design of the plant the integrity of the protection relay communication links to protect from the risks of common cause failure.	4.3.3