New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-CI-09 Component Interface Module Adequacy of Safety Case

Assessment Report: ONR-NR-AR-16-035
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

Westinghouse Electric Company LLC (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 control and instrumentation (C&I). Specifically this report addresses GDA Issue GI-AP1000-CI-09 Revision 0 – Component Interface Module (CIM) – Adequacy of Safety Case**.**

This GDA issue arose in Step 4 because of the need to improve the quality of the CIM Basis of Safety Case (BSC). The key areas identified for improvement were:

- demonstration that the development process for the CIM is compliant or equivalent to International Electrotechnical Commission (IEC) standards; and
- identification of the evidence to support the demonstration.

The Westinghouse GDA issue resolution plan stated that its approach to closing the issue was:

- to provide a revised BSC to address the observations identified in the ONR C&I Step 4 report; and
- to provide key documents in support of the BSC.

My assessment conclusion is that the safety case for the CIM has been significantly improved through the provision of the revised BSC and its references and is adequate for the stage of design presented during GDA.

My judgement is based upon the following factors:

- review of the CIM BSC and key supporting submissions as identified in the resolution plan and the sampling of selected references to these documents;
- adoption by Westinghouse of IEC standards for the safety justification of the CIM and satisfaction of key ONR Safety Assessment Principles (SAPs); and
- the explicit inclusion of compensating measures to provide conformance to IEC standards and SAPs in Westinghouse's CIM BSC safety plan for the development of the CIM post-GDA.

The following matters remain, which are for a future licensee to consider and take forward in its site-specific safety submissions:

- fully develop the safety case outlined in the CIM BSC (for example, by implementing the safety plan therein) as the detailed design and implementation of the system is completed post GDA;
- implement the compensating measures identified in the standards compliance submissions (addressing all relevant clauses) by, for example, including design and implementation detail such as verification, validation and commissioning test records; and
- ensure that the techniques utilised for the verification of the CIM meet recognised good practice and cover the full scope of the system development.

These matters do not undermine the generic design safety submission provided by Westinghouse. Resolution will require licensee input/decision.

In summary, I am satisfied that GDA Issue GI-AP1000-CI-09 Revision 0 – CIM – Adequacy of Safety Case can be closed.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
CAE	Claims, Arguments and Evidence
BSC	Basis of Safety Case
C&I	Control and Instrumentation
CIM	Component Interface Module
DAC	Design Acceptance Confirmation
ESF	Engineered Safety Feature
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IEC	International Electrotechnical Commission
LOC	Lines of Code
MCDC	Modified Condition Decision Coverage
MDEP	Multinational Design Evaluation Programme
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
pfd	Probability of failure on demand
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PSA	Probabilistic Safety Assessment
RGP	Relevant Good Practice
RP	Requesting Party
RQ	Regulatory Query
SAPs	Safety Assessment Principles
SSC	System, Structure (and) Component
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor
US NRC	United States 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 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 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 for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically this report addresses GDA Issue GI-AP1000-CI-09 Revision 0 – CIM – Adequacy of Safety Case.

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. Further information on the GDA process in general is also available on our website (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-14-001 Rev. 0 (Ref. 14).

5. The scope of assessment focused on the following aspects of the Westinghouse Component Interface Module (CIM) safety case:

   - the basis of safety case (BSC) for the CIM (Ref. 11), which is the key submission addressing the related GDA Issues (Action: GI-AP1000-CI-09.A2); and
   - the sampling of key references to the BSC, including those identified in the Westinghouse resolution plan (Ref. 2).

6. My assessment addressed the need to improve the quality of the CIM safety case through the submission of a BSC and supporting references, this being the key area of concern identified during GDA Step 4. The GDA submission needs to be consistent with that of a Pre-Construction Safety Report (PCSR) but the Step 4 submissions fell short of ONR expectations in this regard.

7. The scope of my assessment was appropriate for GDA because it ensured an adequate safety justification had been set out prior to the detailed design and implementation of the CIM, thereby reducing the risk that significant safety issues will arise post-GDA. The scope of assessment was proportionate since it provided a review of the detail expected of a PCSR and supporting references such as the CIM BSC (see ONR Guidance to Requesting Parties - http://www.onr.org.uk/new-reactors/ngn03.pdf). In addition, my assessment focussed on the key areas that Westinghouse needed to address in order to close out the GDA issue.

1.3 Method

8. This assessment complies with internal guidance on the mechanics of assessment within ONR as described in ONR guide NS-PER-GD-014 Revision 5 (see Ref. 1).

1.3.1 Sampling Strategy

9. It is rarely possible or necessary to assess a safety submission in its entirety, and therefore ONR adopts an assessment strategy of sampling. The sampling strategy for this assessment was to review the CIM BSC (Ref. 11) and sample key references identified in the Westinghouse resolution plan (Ref. 2) and CIM BSC.

10. I included a review of the BSC to confirm that it meets the expectations outlined in the GDA issue and relevant guidance. I also consider it important that the BSC and supporting submissions demonstrate conformance to ONR Safety Assessment Principles (SAPs) and key relevant good practice nuclear C&I standards. I included specific sampling of submissions in these areas in my review.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

11. ONR's GDA Guidance to Requesting Parties (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) 51 sets out regulatory expectations for a PCSR (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 CC-02 (Ref. 20), requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence (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 CC-02, and therefore this report does not discuss the C&I aspects of the PCSR. This assessment focused on the supporting documents and evidence specific to GDA Issue GI-AP1000-CI-09 Revision 0, CIM – Adequacy of Safety Case.

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment are principally the SAPs (Ref. 8), internal TAGs (Ref. 9), relevant national and international standards, and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. Further detail is provided in the following subsections.

2.2.1 Safety Assessment Principles

15. The key SAPs I used to support my assessment are provided in Table 1. Note that the full scope of SAPs applicable to C&I assessment as considered during GDA Step 4 can be found in the Step 4 C&I assessment report (Ref. 10, Table 4).

Table 1: Key Safety Assessment Principles

ECS.3	Standards
EDR.1	Failure to safety
EDR.2	Redundancy, diversity and segregation
EQU.1	Qualification procedures
ERL.1	Form of claims
ERL.2	Measures to achieve reliability
ESS	All ESS SAPS, since the CIM is a safety system and is Class 1 as defined in IEC 61226. In particular, the ESS SAPs listed below.
ESS.5	Plant interfaces
ESS.15	Alteration of configuration, operational logic or associated data

ESS.20	Avoidance of connections to other systems
ESS.21	Reliability
ESS.27	Computer-based safety systems

2.2.2 Technical Assessment Guides

16. The TAGs that have been used to support this assessment are set out in Table 2.

Table 2: Technical Assessment Guides

NS-TAST-GD-003 (Rev. 7)	Safety Systems
NS-TAST-GD-046 (Rev. 3)	Computer Based Safety Systems – relevant since it defines the concept of production excellence and independent confidence-building measures

2.2.3 National and International Standards and Guidance

17. The international standards and guidance that have been used to support this assessment are set out in Table 3 (see Ref. 16 for details of the standards).

Table 3: National and International Standards and Guidance

IEC 61226:2009	Nuclear power plants, Instrumentation and control systems important to safety, Classification of instrumentation and control functions. International Electrotechnical Commission (IEC).
IEC 61513:2011	Nuclear power plants, Instrumentation and control for systems important to safety, General requirements for systems. IEC.
IEC62566: 2012	Nuclear power plants, Instrumentation and control for systems important to safety, Development of HDL-programmed integrated circuits for systems performing Category A functions. IEC.
IEC 60987:2007 + A1:2013	Nuclear power plants, Instrumentation and control important to safety, Hardware design requirements for computer-based systems. IEC.
IAEA NP-T-3.17	Technical Report NP-T-3.17, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants. IAEA.

2.3 Use of Technical Support Contractors

18. It is usual when performing a GDA for ONR to use technical support contractors (TSCs); 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 etc.

19. Table 4 sets out the broad areas in which ONR utilised technical support for this assessment. ONR required this support to provide additional capacity and access to independent advice and experience. The TSC support enabled ONR to address the peak load of assessment required by the Westinghouse submission programme.

20. The TSC used for all work packages was Altran UK Ltd.

Table 4: Work Packages Undertaken by the TSC

TSC	Work Package
Altran	Review of UKP-PMS-GLR-002 Rev. 2, United Kingdom AP1000 Component Interface Module Safety Case Basis (Ref. 11), plus sampling of selected BSC references
Altran	Review of UKP-PMS-GLR-004 Rev. 0, United Kingdom AP1000 Component Interface Module Safety Assessment Principles (Ref. 4) and key references
Altran	Review of UKP-PMS-GLR-008 Rev. 1, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the PMS Component Interface Module (Ref. 5) and key references
Altran	Review of UKP-PMS-GLR-005 Rev. 2, United Kingdom AP1000 IEC 60987 Compliance Assessment for the PMS Component Interface Module (Ref. 6) and key references
Altran	Review of UKP-PMS-GLR-006 Rev. 1, United Kingdom AP1000 IEC 62566 Compliance Assessment for the PMS Component Interface Module (Ref. 7) and key references

21. The TSC undertook the technical reviews under the close direction and supervision of ONR. The regulatory judgement on the adequacy or otherwise of the **AP1000** design was made exclusively by ONR. ONR raised all Regulatory Queries (RQs) and meeting actions with Westinghouse. RQs are requests by ONR for clarification and additional information and are not necessarily indicative of any perceived shortfall. The location of all RQs (for example, RQ-AP1000-xxxx, where xxxx is the unique identifier number) in ONR's document management system (i.e. TRIM) can be identified through Ref. 13.

22. The TSC provided a report (Ref. 15) that addresses the scope of work listed above. The TSC also reviewed responses to RQs and meeting actions placed on Westinghouse. The TSC report includes a summary statement of the results of its work and findings (i.e. Technical Observations (TOs)). I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under assessment findings (see below and Annex 1). The TSC TOs provide further guidance on the GDA assessment findings and their means of resolution. Within my report I have provided references to the TSC TOs contained in Ref. 15 using the unique TO identifiers (e.g. CI-xx.TO8-mmmm.nn, where mmmm is the Ref. 15 report section containing the TO).

2.4 Integration with Other Assessment Topics

23. 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.

24. I recognised the need to consult with other inspectors at various stages of my assessment. Similarly, there were occasions where other assessors sought my input to support their own assessment. I considered these interactions to be very important for the success of the project, particularly my interactions with the Probabilistic Safety Assessment (PSA) and Fault Studies disciplines, for example I consulted with the ONR:

- PSA inspector concerning the reliability claims used within Westinghouse probability calculations.
- Mechanical engineering inspector concerning the interface of the CIM with mechanical items of plant.
- Fault studies inspector concerning the contents of the Westinghouse fault schedule and faults addressed by actuations requiring correct CIM operation.

25. The only cross-cutting issue that was of specific relevance to this assessment was GI-AP1000-CC-02, concerning the production of a revised PCSR, which is discussed in Section 2.1 of this report.

2.5 Out of Scope Items

26. For each system important to safety within the scope of GDA, Westinghouse identified the scope of the lifecycle documents available for assessment. This information is documented within Section 2.3.5 of the ONR Step 4 C&I assessment report (Ref. 10). The availability of documents for each lifecycle phase was allocated to one of three categorises, as follows:

- A – all evidence for that stage of development is complete and will be available to ONR for assessment.
- B – the documentation that specifies the process for that phase will be available but not all the output products (e.g. documents and reports) from that phase will be available to ONR for assessment.
- C – neither the documentation that specifies the process nor the output products for that phase will be available to ONR for assessment.

27. The CIM is a subsystem within the Protection and Safety Monitoring System (PMS), and Table 5 identifies the availability of supporting documentation for the lifecycle phases of this system.

Table 5: Availability of PMS (CIM) Documentation for GDA Assessment

Lifecycle Phase	PMS (CIM)
Design Requirements	A
System Definition	A*

Design	B
Implementation	B
Test	B
Installation	C

Note – A* denotes some documents will be missing.

28. Recognising that the development of the CIM will only be completed post-GDA, I considered this level of detail to be acceptable to support my assessment.

29. It should be noted that a number of assessment findings associated with the CIM were identified in the ONR Step 4 C&I assessment report (Ref. 10). It is the responsibility of the licensee to demonstrate closure of assessment findings. I have therefore not considered the closure of those associated with the CIM in this assessment. The licensee should, however, consider the Westinghouse submissions in this area when making the case for closure of these assessment findings post GDA.

3 REQUESTING PARTY'S SAFETY CASE

30. The Westinghouse safety case addressing the shortfalls identified in GDA Issue GI-AP1000-CI-09 is documented within the CIM BSC (Ref. 11) and supporting documents. I identified the following key supporting documents:

- UKP-PMS-GLR-004, United Kingdom AP1000 Component Interface Module Safety Assessment Principles Report (Ref. 4)
- UKP-PMS-GLR-008, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the PMS Component Interface Module Report (Ref. 5)
- UKP-PMS-GLR-005, United Kingdom AP1000 IEC 60987 Compliance Assessment for the PMS Component Interface Module (Ref. 6)
- UKP-PMS-GLR-006, United Kingdom AP1000 IEC 62566 Compliance Assessment for the PMS Component Interface Module (Ref. 7)

31. In response to my requests for detailed supporting design documents, Westinghouse also supplied additional evidential documentation (such as requirement specifications, test reports, independent verification and validation plans etc.). A comprehensive list of these documents is provided in the references section of the TSC report (Ref. 15).

32. I consider the BSC (Ref. 11) to be the prime safety case reference for the CIM. I found that the BSC addressed the following topics:

- The high-level claims on the CIM, the relevant industry standards, and an overview of the supporting documentation.
- The context of the CIM BSC in relation to the PCSR, other BSCs, and the CIM CAE documentation.
- A system description.
- A safety plan which describes those system development and safety justification activities that will take place post GDA. The plan includes how and when Westinghouse will implement the compensating measures identified in its standards conformance assessments (such as by including design and implementation detail).
- A high-level demonstration of conformance to a safety lifecycle based on that defined in IEC 61513.
- Those activities supporting the CIM safety lifecycle. This includes an overview of compliance with the SAPs and industry standards as well as a description of the Westinghouse quality management system as applied to the CIM.
- The ALARP case for the CIM.
- The approach taken to address GDA Step 4 TOs.

33. My assessment of the BSC (Ref. 11) is captured in Section 4.2 of this report.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-09

34. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, Purpose and Scope of Permissioning (Ref. 1).

4.1 Scope of Assessment Undertaken

35. The scope of my assessment covered the Westinghouse submissions identified in the GDA Issue resolution plan (Ref. 2). This included the CIM BSC (Ref. 11) and supporting references, as outlined in Section 3 of this report.

36. The submissions made by Westinghouse in this topic area (see Section 3 for details) may address some of the outstanding GDA Step 4 assessment findings (see Ref. 10). However, it is the responsibility of the licensee to demonstrate closure of the Step 4 assessment findings. The licensee should consider these submissions where relevant when making the case for closure of the assessment findings.

37. It should be noted that the adequacy of the overall PMS safety justification was the subject of a separate assessment (see Ref. 19).

4.2 Assessment

4.2.1 Background

38. My assessment of Westinghouse's submissions provided in response to GDA Issue GI-AP1000-CI-09 is described below. The submissions were reviewed and I raised requests for clarification in RQs. As appropriate, the submitted documents were revised by Westinghouse to address these requests.

39. The description of the scope of work performed by the TSC, and the TOs arising from its work, are contained in a TSC report (Ref. 15).

40. My assessment was performed in accordance with my assessment plan (Ref. 14).

41. In order to provide context to the assessment I performed, I have provided a general description of the function of the CIM in the following subsection.

4.2.2 Component Interface Module Description

42. The CIM is a subsystem of the PMS which is the primary protection system for the **AP1000** plant. As such the PMS principally fulfils reactor trip and engineered safety feature (ESF) actuation functions. The CIM provides the PMS interface to the field components (such as valves, circuit breakers) for the ESF actuation functions. It also receives commands for these same field components from the Class 2 plant control system (PLS). The CIM arbitrates between PMS and PLS demands, while prioritising the PMS signals.

43. The CIM design is implemented using field-programmable gate array (FPGA) technology.

44. The ESF actuation functions initiated through the CIM are designated Category A in accordance with IEC 61226, and are associated with functions such as residual heat removal following reactor trip. The PMS, incorporating the CIM subsystem, is classified as a Class 1 system in accordance with IEC 61513. The reliability claim for the PMS (including the CIM) is 1E-3 probability of failure on demand (pfd).

45. The CIM subsystem was originally developed based on US Nuclear Regulatory Commission (NRC) Regulatory Guides that endorse Institute of Electrical and Electronics Engineers (IEEE) industry standards. However, within the UK the relevant

good practice (RGP), as reflected in ONR SAPs, is based upon the IEC international nuclear sector standards, the lead standard being IEC 61513. I used this group of IEC standards to inform my assessment (see Table 3).

46. Westinghouse produced a CIM BSC document (Ref. 11), accompanied by relevant supporting documents (Refs 4, 5, 6 and 7), with the purpose of providing arguments and evidence for the safety case claims made for the CIM within the UK **AP1000** safety case. Evidence was presented to support claims such as:

- compliance with relevant IEC nuclear sector standards, such as IEC 61513;
- operation with a reliability of 1E-3 pfd or better; and
- conformance to applicable UK ONR SAPs, namely those applicable to a Class 1 C&I system.

47. The outcome of my assessment of the CIM safety case CAE, as provided in the Westinghouse safety case, is documented in this report.

4.2.3 GDA Issue GI-AP1000-CI-09 Actions

48. Two actions were raised under this issue in the GDA Step 4 C&I assessment report (Ref. 10):

- GDA Issue Action GI-AP1000-CI-09.A1 – Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the CIM
- GDA Issue Action GI-AP1000-CI-09.A2 – Westinghouse to provide a basis of safety case for the completed design of the CIM

49. In response to Action GI-AP1000-CI-09.A1, Westinghouse made all necessary CIM documents available to ONR in the UK. Westinghouse submitted the formal documents identified in the resolution plan as they became available and in accordance with the rescheduled submission programme. Westinghouse submitted further supporting documents to ONR following RQ requests.

50. As a result of the access to documentation provided in the UK, I consider that action GI-AP1000-CI-09.A1 has been satisfactorily addressed (for further detail, see Section 4.2.4).

51. Regarding Action GI-AP1000-CI-09.A2, ONR outlined its expectations of the topics and elements of a BSC in GDA Issue GI-AP1000-CI-09 and in the ONR C&I GDA Issues Closure Guidance Document (Ref. 12). I supplied Ref. 12 to Westinghouse as additional guidance on the content of BSCs. In the letter supplying this guidance (Ref. 3), I explained that it is the requesting party's responsibility to consider and provide a comprehensive safety submission addressing each of the GDA issues.

52. In response to this action, Westinghouse provided a BSC document (Ref. 11). The detail of the CAE for conformance to the SAPs and relevant standards is not contained in the BSC but is provided in separate documents referenced therein (Refs 4, 5, 6 and 7). My assessment of these documents is described in Section 4.2.4.

53. I found (Ref. 15) that the structure and content of the CIM BSC (Ref. 11), together with the key supporting references, broadly met my expectations in terms of BSC topics and elements as outlined in the GDA issue and supporting guidance.

54. Commitments have been made by Westinghouse in the BSC safety plan (Ref. 11) that the BSC and supporting references will be updated post GDA to provide further conformance demonstrations as the CIM development programme proceeds. I am content that this approach is appropriate, as such demonstrations require evidence that will only become available later.

55. I therefore judge that action GI-AP1000-CI-09.A2 has been satisfactorily addressed (for further detail, see Section 4.2.4).

4.2.4 Assessment

56. I assessed the adequacy of the overall safety case as captured by the BSC (Ref. 11), the supporting documents (Refs 4, 5, 6 and 7) and their references. I reviewed the submissions and raised clarification requests by RQ. As appropriate, Westinghouse revised the submitted documents to address the RQs.

57. My overall assessment was informed by the guidance in an International Atomic Energy Agency (IAEA) technical report, which considered the application of FPGAs in instrumentation and control systems of nuclear power plants (Ref. 18). The report advises that FPGAs should be considered to have a lower complexity than microprocessor solutions. I particularly noted the information presented in Figure 5 of the technical report, which shows that the type of FPGA technology proposed for the UK CIM is considered to be only marginally more complex than conventional hardware designs. I also noted, from the Westinghouse response to RQ-AP1000-1711, the relatively modest quantity of code within each CIM (estimated to be around 7000 lines of code) when compared with a software-based reactor protection system.

58. I have provided a summary of my assessment in the following paragraphs.

59. I assessed the adequacy of the claim of compliance with ONR SAPs (Ref. 8). The main supporting document provided by Westinghouse to support this claim was UKP-PMS-GLR-004, United Kingdom AP1000 Component Interface Module Safety Assessment Principles (Ref. 4).

60. I reviewed the list of SAPs that Westinghouse had determined were relevant to the CIM, to ensure that the scope of the Westinghouse submission was adequate. I noted that a number of SAPs relevant to the CIM were not considered within Ref. 4 but, as they were considered within the relevant overall PMS documentation (see Ref. 19) and the CIM is a subsystem of the PMS, I concluded that this approach was acceptable.

61. Westinghouse presented the case for compliance with SAPs in a structured CAE style. Westinghouse generally provided a top-level claim for each SAP, which was essentially a restatement of the SAP, sitting below this top-level claim a number of sub-claims were provided. For each sub-claim Westinghouse provided an argument that generally made reference to supporting evidential documents.

62. I considered the assessment against SAP ESS.27 to be of particular importance for the CIM, as it is implemented using complex hardware, namely FPGA technology. I noted that the SAP recommendation (Ref. 8) that the testing programme should be subject to independent review was not explicitly addressed. I have included a recommendation that this item be reconsidered post GDA in TO2.2.2.3.4.3-3 within Assessment Finding CP-AF-AP1000-CI-019 (see paragraph 81).

63. I considered the evidence provided by Westinghouse to support claims of production excellence (see NS-TAST-GD-046 – Ref. 9) through compliance with three international standards, namely:

- IEC 61513 – Nuclear power plants – Instrumentation and control important to safety – General requirements for systems;
- IEC 60987 – Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems; and
- IEC 62566 – Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing Category A functions.

64. I was content that these standards were appropriate to support this claim of production excellence as I consider the suite of standards associated with IEC 61513 (which includes IEC 60987 and IEC 62566) to effectively represent UK relevant good practice.

65. Although I generally found the case presented by Westinghouse to be adequate and sufficient to support GDA issue closure, I identified some areas of potential improvement. These are typically associated with providing greater clarity of CAE, and I have captured them in the TOs referenced within Assessment Finding CP-AF-AP1000-CI-019 (see paragraph 81).

66. During the course of my assessment, I raised RQs where I was concerned that there were weaknesses in the safety case, where there was a lack of clarity, or where other relevant concerns came to my attention (such as international operational experience as reported in paragraph 68 of this report). I raised RQs in connection with the BSC itself, the SAPs compliance assessment and in connection with claims of standards conformance. A summary of the more significant RQs relevant to my assessment is provided below (see Ref. 17 for further detail).

RQ-AP1000-1367 – Comments on United Kingdom AP1000 IEC 60987 Compliance Assessment for the PMS Component Interface Module

67. I raised this RQ against the IEC 60987 compliance document (Ref. 6) following a Level 4 meeting I had had with Westinghouse where I had raised preliminary comments. The topics covered by this RQ concerned issues such as the clarity of references to particular clauses within the IEC standard, the categorisation of clauses within the standard as being or not being relevant requirements that should be addressed, and the justification of the adequacy of compensating measures. Westinghouse revised Ref. 6 to address my comments.

RQ-AP1000-1434 – Comments on AP1000 IEC 62566 Compliance Assessment for the PMS Component Interface Module

68. I raised this RQ against the IEC 62566 compliance document (Ref. 7) to highlight issues such as the clarity of evidence supporting claims of compliance with specific clauses within IEC 62566, the terminology used within the document, the need to address all relevant clauses, and the clarity of the lifecycle definition. Westinghouse revised Ref. 7 to address the issues I had raised. I also raised RQ-AP1000-1707 (see below) as a result of this assessment, to document the generic issue of the need for the C&I safety case to adequately address all pertinent clauses within relevant standards.

RQ-AP1000-1559 – CIM Module Failures

69. I raised this RQ following receipt of operational feedback through my involvement in the Multinational Design Evaluation Programme (MDEP, an international regulators' forum focused on the assessment of new reactor designs). It came to my attention at an MDEP meeting (see Ref. 21) that CIM modules in reactors outside of the UK had

been subject to a particular type of failure. The Westinghouse response to RQ-AP1000-1559 explained the differences in design between the modules in question and those intended for use in the UK. This provided me with sufficient confidence that the UK design of CIM would not be susceptible to the type of failure that had been reported.

RQ-AP1000-1583 – CIM IEC 60987 Compliance Document Review of Responses to RQ-AP1000-1367

70. The Westinghouse IEC 60987 compliance document was revised following the queries I raised under RQ-AP1000-1367 (see above). I raised RQ-AP1000-1583 following my review of the revised document, to capture queries covering issues such as the adequacy and clarity of information addressing CAE for hardware performance. Westinghouse subsequently revised the document again to address my concerns.

RQ-AP1000-1707 – Treatment of 'Should' and 'May' Clauses in Standards Compliance Reviews

71. I found in my review of all of the standards compliance documents (Refs 5, 6 and 7) that the treatment of the requirements of the standards varies. I found that only 'shall' statements are provided with a full CAE trail with gaps and compensating measures identified where necessary. I found that 'may' and 'should' statements are either not addressed or do not have gaps or compensating measures identified. I found that a similar approach was taken across all of the standards conformance demonstrations for all of the **AP1000** C&I systems subject to GDA.

72. I raised generic RQ-AP1000-1707, requesting Westinghouse to address fully all 'may' and 'should' clauses and sub-clauses in standards conformance assessments, or, if this is not considered reasonably practicable, to provide a full justification for the position taken. I extended this request to all of the C&I systems as it is necessary for these informative aspects of relevant standards to be considered to determine whether adequate measures have be taken to reduce risks as low as is reasonably practicable (ALARP) for these systems.

73. In the response to RQ-AP1000-1707, Westinghouse committed to update the standards conformance documents, such that 'should' and 'may' clauses, and statements in which there is no compliance assessment, or in which there is no compensating measure identified for a gap in compliance, will be completed. Westinghouse stated that this commitment would be addressed under Step 4 Assessment Finding AF-AP1000-CI-005, which states:

> The licensee shall produce a comprehensive demonstration of compliance with the five level 1 IEC nuclear sector C&I standards (i.e. BS IEC 61226, BS IEC 61513, BS IEC 60987, BS IEC 60880 and BS IEC 62138) for the **AP1000** C&I Systems Important to Safety (SIS). The demonstration shall address: all relevant clauses; the operation and maintenance part of the SIS lifecycle; platforms and systems individually; and Class 3 systems. For further guidance see T14.TO1.01, T14.TO.03 and T14.TO2.04 in Annex 4, and T16.TO2.05 and T16.TO2.10 in Annex 6.

74. It should be noted that it is the responsibility of the licensee to demonstrate closure of assessment findings. However, the licensee should consider the Westinghouse submissions in this area when making the case for closure of the assessment findings.

75. The detailed findings from my review of the standards compliance documents (Refs. 5, 6 and 7) are not captured within AF-AP1000-CI-005. I have therefore raised Assessment Finding CP-AF-AP1000-CI-010, to be read in conjunction with AF-AP1000-CI-005, in order that the licensee fully addresses all 'should' and 'may'

statements in all standards conformance assessments for the CIM. If the licensee considers this not to be reasonably practicable it should provide a full justification for the position taken.

> **GDA Assessment Finding: CP-AF-AP1000-CI-010** – The licensee shall address all 'should' and 'may' statements in all standards conformance assessments for the CIM.
>
> For further guidance on this assessment finding, see also Step 4 Assessment Finding AF-AP1000-CI-05 and TOs CI-09-TO2-2.2.2.3.3-2 and CI-09-TO2-2.2.3.3.4-1 in Ref. 15.

RQ-AP1000-1711 – Comments on AP1000 CIM BSC

76. I raised a number of queries under this RQ covering issues including the reasonable practicability of applying the modified condition decision coverage (MCDC) testing technique in the CIM verification and validation activities. Such a technique would provide more extensive code coverage than those techniques currently proposed.

77. The Westinghouse response to this particular query argued that MCDC testing is not applicable for FPGA code. No argument was provided to demonstrate why MCDC is not reasonably practicable for the CIM, nor was there an identification of the type of gaps (i.e. potential faults) that would remain if MCDC testing were not undertaken. I have therefore included the need to further consider relevant good practice testing techniques post GDA within Assessment Finding CP-AF-AP1000-CI-019 (see paragraph 81).

78. I also queried the adequacy of the verification techniques proposed for the final steps in the development of the CIM FPGAs (i.e. the steps where the place and route netlist is converted into a bitstream, and subsequently programmed onto the FPGA device).

79. The Westinghouse response to this query, as well as a presentation provided earlier in GDA (Ref. 22), stated that testing (in particular black box testing) of the configured FPGA device would provide adequate verification. There is a risk of errors being introduced during the development steps mentioned above, and it is not clear if the test coverage achieved during the black box testing is adequate, or if all reasonably practicable measures have been taken, to detect such errors. I have therefore included the need to further consider the reasonable practicability of additional verification techniques for the latter phases of the FPGA development lifecycle in Assessment Finding CP-AF-AP1000-CI-019 (see paragraph 81).

RQ-AP1000-1712 – Comments on AP1000 CIM IEC 61513 Compliance

80. I raised this RQ against the IEC 61513 compliance document (Ref. 5) to document issues such as the extent of signal filtering within the design, the extent of dual redundant operation within the communications architecture and the clarity of some text relating to electromagnetic interference susceptibility. In response, Westinghouse provided further justifications and clarifications and revised Ref. 5.

RQ-AP1000-1713 – Comments on AP1000® CIM Safety Assessment Principle Evaluation

81. I raised this RQ against Ref. 4 to document issues such as the need for the CIM to achieve 'failure to a safe condition' under all circumstances, the extent of error detection within the design, and the rationale for proposed actions in the event of errors being detected. In response, Westinghouse provided further justifications and clarifications. I reviewed this response and noted that a number of minor points remained. I have captured these points in the TOs referenced in Assessment Finding

CP-AF-AP1000-CI-019 below. In conclusion I judge that there are no outstanding issues associated with SAP compliance that would preclude closure of the GDA issue.

82. The safety case documentation (including the BSC and conformance assessments etc.) will be updated as the detailed design of the CIM is implemented post-GDA (for example, to document implementation of the compensating measures identified in the safety plan). Notwithstanding this further work, the implementation detail for the CIM design presented during GDA is sufficient to demonstrate that no significant safety issues remain. I am content that it is appropriate to implement the conformance demonstration compensating measures post GDA as they require the provision of evidence that will become available at that time. I have included the requirement to develop the safety case fully and to implement the safety plan, as the development of the CIM progresses, in Assessment Finding CP-AF-AP1000-CI-019 below:

> **GDA Assessment Finding: CP-AF-AP1000-CI-019** – The licensee shall fully develop the safety case outlined in the CIM BSC and its supporting documents and implement the BSC safety plan (Ref. 11). This shall include but not be limited to:
>
> - Implement the compensating measures, including those in the standards compliance assessments.
> - Ensure that the techniques utilised for the verification of the CIM meet recognised good practice and justify:
>   - the extent of code coverage achieved through their application; and
>   - that adequate coverage of the whole FPGA development lifecycle is achieved.
>
> For further guidance on the completion of the CIM safety case, see Technical Observations CI-09-TO2-2.2.2.3.3-1 and -3, CI-09-TO2-2.2.2.4.2.6-1, CI-09-TO2-2.2.2.4.2.13-1, CI-09-TO2-2.2.2.4.3-1 to -5, GI-09-TO2.2.2.3.4.2.8-1 and CI-09-TO2-2.2.3.4.3-1 to -3 in Ref. 15.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

83. My assessment has included a sample-based assessment of the compliance of the Westinghouse CIM submissions with relevant standards, guidance and good practice. This assessment is described in the section 4.2.4. I am content that Westinghouse has made satisfactory use of relevant standards, guidance and good practice.

4.4 Assessment Findings

84. During my assessment, two assessment findings were identified for a future licensee to take forward in their site-specific safety submissions, namely CP-AF-AP1000-CI-010 and CP-AF-AP1000-CI-019. Details of these findings are provided in Section 4.2.4 and in Annex 1.

85. These findings 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.

86. 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; or
- to resolve this matter, the level of detail of the design needs to be beyond what can reasonably be expected in GDA (e.g. manufacturer/supplier input is required; or areas where the technology changes quickly, and so to avoid obsolescence of design).

87. It should be noted that the resolution of GDA Step 4 assessment findings has not been considered in my assessment since they are defined as requiring resolution by the licensee.

5 CONCLUSIONS

88. This report presents the findings of the assessment of GDA Issue GI-AP1000-CI-09 Revision 0 CIM – Adequacy of Safety Case, relating to the **AP1000** GDA closure phase.

89. My assessment has included consideration of whether the Westinghouse submissions for this GDA issue meet the expectations of relevant SAPs, standards, guidance and good practice (see Tables 1, 2 and 3).

90. To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the submissions provided by Westinghouse in response to GDA Issue GI-AP1000-CI-09 Revision 0 CIM – Adequacy of Safety Case.

91. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-09 may be closed.

6 REFERENCES

1. ONR, HOW2 Guide NS-PER-GD-014 Rev 5, Purpose and Scope of Permissioning. www.onr.org.uk/operational/assessment/index.htm
2. Westinghouse GDA Resolution Plan for GI-AP1000-CI-09, CIM – Adequacy of Safety Case, Rev 3. TRIM 2016/92108
3. ONR-WEC-0006N, C&I GDA Issues Closure Guidance Document Covering Letter. TRIM 2015/84411
4. UKP-PMS-GLR-004 Rev 0, United Kingdom AP1000 Component Interface Module Safety Assessment Principles. TRIM 2016/286240
5. UKP-PMS-GLR-008 Rev 1, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the PMS Component Interface Module. TRIM 2016/466199
6. UKP-PMS-GLR-005 Rev 2, United Kingdom AP1000 IEC 60987 Compliance Assessment for the PMS Component Interface Module. TRIM 2016/378483
7. UKP-PMS-GLR-006 Rev 1, United Kingdom AP1000 IEC 62566 Compliance Assessment for the PMS Component Interface Module. TRIM 2016/169654
8. ONR, Safety Assessment Principles for Nuclear Facilities 2014. (www.onr.org.uk/saps/saps2014.pdf)
9. ONR, Technical Assessment Guides. (www.onr.org.uk/operational/tech_asst_guides/index.htm)
10. ONR-GDA-AR-11-006 Rev 0, Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor – Assessment Report. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf
11. UKP-PMS-GLR-002 Rev 2, United Kingdom AP1000 Component Interface Module Safety Case Basis. TRIM 2016/466185
12. C&I GDA Issues Closure Guidance Document Rev 0. TRIM 2015/84414
13. ONR RQ Tracking Sheet. TRIM 2016/383615
14. ONR-GDA-AP-14-001 Rev 0, AP1000 GDA C&I Assessment Plan. TRIM 2015/149263
15. Altran S.P1641.40.TSC267.7 Issue 1, ONR/T2723: Review of Submissions for the Closure of GDA Issue 09 CIM – Adequacy of Safety Case. TRIM 2017/81316
16. International Electrotechnical Commission. www.iec.ch/
17. ONR **AP1000** GDA Regulatory Queries (RQs) and Responses. TRIM 4.4.1.2541.
18. IAEA Technical Report NP-T-3.17, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants. www.iaea.org/
19. ONR-NR-AR-16-034 Rev 0, GDA Issue GI-AP1000-CI-08 – PMS Adequacy of Safety Case. TRIM 2016/274946
20. GDA Issue CC-02, Rev 3, PCSR to Support GDA. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf
21. ONR-NR-CR-16-10 Rev 0, ONR Contact Record, MDEP Digital Instrumentation and Control (DI&C) Working Group Meeting, April 2016. TRIM 2016/146415
22. NPP_JNE_000669 Enclosure 1, Atkins presentation – AP1000 GDA, CIM Static Analysis as ICBM, February 2016. TRIM 2016/58655

Annex 1:

Assessment Findings to be addressed during the Forward Programme – Control and Instrumentation

Assessment Finding Number	Assessment Finding	Report Section Reference
CP-AF-AP1000-CI-010	The licensee shall address all 'should' and 'may' statements in all standards conformance assessments for the CIM. For further guidance on this assessment finding, see also Step 4 Assessment Finding AF-AP1000-CI-05 and TOs CI-09-TO2-2.2.2.3.3-2 and CI-09-TO2-2.2.3.3.4-1 in Ref. 15.	4.2.4
CP-AF-AP1000-CI-019	The licensee shall fully develop the safety case outlined in the CIM BSC and its supporting documents and implement the BSC safety plan (Ref. 11). This shall include but not be limited to: • Implement the compensating measures, including those in the standards compliance assessments. • Ensure that the techniques utilised for the verification of the CIM meet recognised good practice and justify: - the extent of code coverage achieved through their application; and - that adequate coverage of the whole FPGA development lifecycle is achieved. For further guidance on the completion of the CIM safety case, see Technical Observations CI-09-TO2-2.2.2.3.3-1 and -3, CI-09-TO2-2.2.2.4.2.6-1, CI-09-TO2-2.2.2.4.2.13-1, CI-09-TO2-2.2.2.4.3-1 to -5, GI-09-TO2.2.2.3.4.2.8-1 and CI-09-TO2-2.2.3.4.3-1 to -3 in Ref. 15.	4.2.4