New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-CI-08 – PMS Adequacy of Safety Case

Assessment Report: ONR-NR-AR-16-034
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

Westinghouse Electric Company LLC (Westinghouse) is the reactor design company for the **AP1000®** pressurised water 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-08 Revision 0 – PMS Adequacy of Safety Case.

This GDA issue arose in Step 4 due to the need to improve the quality of the Protection and Safety Monitoring System (PMS) safety justification.

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

- provide a Basis of Safety Case (BSC) for the PMS that met ONR expectations;
- submit key documents in support of the BSC; and
- make available further documents that support the BSC as requested by ONR.

My assessment conclusion is that the safety case for the PMS has been significantly improved through the provision of the 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 PMS BSC and key supporting submissions as identified in the resolution plan and the sampling of selected references to these documents;
- adoption by Westinghouse of International Electrotechnical Commission (IEC) standards for the safety justification of the PMS and satisfaction of key ONR SAPs; and
- the explicit inclusion of compensating measures to provide conformance to IEC standards and SAPs in Westinghouse's PMS BSC safety plan for the development of the PMS 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 PMS BSC (including, for example, implementation of the safety plan therein) as the detail design and implementation of the system is completed post GDA.
- Implement the compensating measures identified in the SAPs and standards compliance submissions (addressing all relevant clauses) by, for example, including design and implementation detail such as verification, validation and commissioning test records.
- Complete the substantiation of the adequacy of the Common Q platform (including, for example, operating systems and programmable complex electronic components (PCECs)).
- Document and justify the reliability of the final as-built PMS design in the safety case.

These matters do not undermine the generic safety submission and require licensee input / decision.

In summary, I am satisfied that GDA Issue GI-AP1000-CI-08 Revision 0 – PMS Adequacy of Safety Case can be closed.

LIST OF ABBREVIATIONS

1oo2	One out of Two
2oo3	Two out of Three
2oo4	Two out of Four
ABB	Asea Brown Boveri
ALARP	As Low As Reasonably Practicable
BSC	Basis of Safety Case
C&I	Control and Instrumentation
CAE	Claims, Arguments and Evidence
CCF	Common Cause Failure
CIM	Component Interface Module
DAC	Design Acceptance Confirmation
DOORS®	Dynamic Object-Oriented Requirements System
EPC	Engineering, Procurement and Construction
ESF	Engineered Safety Feature
FPDS	Flat Panel Display System
FPGA	Field Programmable Gate Array
FQAJ-A	Final Quality Assessment and Justification Report - Addendum
GDA	Generic Design Assessment
IDAC	Interim Design Acceptance Confirmation
IEC	International Electrotechnical Commission
IRWST	In-containment Refuelling Water Storage Tank
ONR	Office for Nuclear Regulation
PCEC	Programmable Complex Electronic Component
PCSR	Pre-Construction Safety Report
PDS	Pre-Developed Software
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
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor

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-08 Revision 0 – PMS 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 my assessment is detailed in assessment plan ONR-GDA-AP-14-001 Rev 0 (Ref. 1).

5. The scope of my assessment focused on the:

   - Basis of Safety Case (BSC) for the PMS (Ref. 2), which is the key submission addressing the GDA issue action GI-AP1000-CI-08.A2; and
   - Sampling of key references to the BSC including those identified in the Westinghouse resolution plan (Ref. 3).

6. My assessment addressed the need to improve the quality of the PMS 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 before the detailed design and implementation of the PMS, thereby reducing the risk that significant safety issues could 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 PMS BSC (see ONR Guidance to Requesting Parties - www.onr.org.uk/new-reactors/ngn03.pdf). In addition, my assessment focused 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 (Ref. 4).

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 PMS BSC and sample key references and supporting submissions identified in the Westinghouse resolution plan and 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 (RGP) nuclear 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) 051 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 GI-AP1000-CC-02 (www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence (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, 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-08 Revision 0 – PMS Adequacy of Safety Case.

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment were principally the SAPs (Ref. 5), internal TAGs (Ref. 6), relevant national and international standards and RGP informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

15. The key SAPs applied within my assessment are included within 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. 7 – Table 4).

Table 1 – Key SAPs

ESS.1 to 27	Engineering principles: safety systems
ECS.2 and 3	Engineering principles: safety classification and standards
EQU.1	Engineering principles: equipment qualification - qualification procedures
EDR.1 to 4	Engineering principles: design for reliability
ERL.1 to 4	Engineering principles: reliability claims
ECM.1	Engineering principles: commissioning - commission testing
EMT.1,3,5,6,7	Engineering principles: maintenance, inspection and testing
ERC.1 to 4	Engineering principles: reactor core

2.2.2 Technical Assessment Guides

16. The TAGs that I have used as part my 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

2.2.3 National and International Standards and Guidance

17. The key international standards and guidance that I have used as part of my assessment are set out in Table 3.

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.
IEC 60880:2009	Nuclear power plants, Instrumentation and control systems important to safety, Software aspects for computer-based systems performing category A functions. IEC.
IEC 60987:2007 + A1:2013	Nuclear power plants, Instrumentation and control systems important to safety, Hardware design requirements for computer-based systems. IEC.

2.3 Use of Technical Support Contractors (TSCs)

18. It is usual in GDA for ONR to use technical support, for example to provide additional capacity to optimise the assessment process, provide access to independent advice and experience, for analysis techniques and models, and enable ONR‘s inspectors to focus on regulatory decision making etc.

19. Table 4 sets out the broad areas in which ONR used 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.

Table 4 – Work Packages Undertaken by the TSC

TSC	Work Package
Altran UK Ltd	Review of PMS BSC (Ref. 2) plus sampling of selected BSC references
“	Review of UKP-PMS-GL-010 Rev 2, United Kingdom AP1000 PMS Safety Assessment Principle Evaluation (Ref. 8) and key references
“	Review of UKP-PMS-GL-012 Rev 1, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the PMS (Ref. 9) and key references
“	Review of UKP-PMS-GL-002 Rev 2, United Kingdom AP1000 IEC 60880 Compliance Matrix for the PMS (Ref. 10) and key references
“	Review of UKP-PMS-GLR-007 Rev 1, United Kingdom AP1000 IEC

	60987 Compliance Matrix for the PMS (Ref. 11)and key references
“	Review of UKP-PMS-GL-005 Rev 1, United Kingdom AP1000 Protection and Safety Monitoring System AC160 Suitability Analysis (Ref. 12) and key references
“	Review of WEG-AR-00579-GEN Rev 00, IEC 60987 Compliance Matrix for the AC160 Product HW as integral part of the Protection and Safety Monitoring System (Ref. 13) and key references
“	Review of GBRA095803 Rev. D, O1-MOD – Qualification Final Quality Assessment and Justification Report – Addendum (Ref. 14) and key references

20. The TSC undertook the technical reviews under the close direction and supervision of ONR. ONR exclusively made the regulatory judgement on the adequacy or otherwise of the **AP1000** reactor. 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 (e.g. RQ-AP1000-xxxx, where xxxx is the unique identifier number) in ONR’s document management system (i.e. TRIM) can be identified through Ref. 22.

21. 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

22. 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. For example I consulted the ONR:

- Probabilistic Safety Assessment (PSA) inspector regarding the modelling of PMS reliability in the PSA;
- fault studies inspector regarding the categorisation of safety functions and the implementation of non- 2 out of 4 (2oo4) voting logic architectures within the PMS; and
- mechanical engineering inspectors regarding the approach taken to plant metrication and the actuation of squib valves within the PMS.

2.5 Out of Scope Items

23. The items that are outside the scope of GDA are identified in the C&I Step 4 assessment report (Ref. 7). Ref. 7 identifies the availability of evidence as follows:

- A - All evidence for that stage of development is complete and available to ONR for assessment;

- B - The documentation that specifies the process for that phase is available but not all the output products (e.g. documents and reports) from that phase are available to ONR for assessment;

- C - Neither the documentation that specifies the process nor the output products for that phase are available to ONR for assessment.

24. For the PMS platform (i.e. the “Common Q” series equipment) it was noted that the “Platform Description” is “A” and “Platform Qualification” is A*, where A* was defined as “The following Common Q components are not qualified to Category A / Class 1 standards: DP620, AI687, AI688, CI631, CI527 and flat panel displays”.

25. In relation to the implementation of the PMS, Westinghouse’s declared availability of documentation for GDA assessment (see Ref. 7) is as shown in Table 5.

Table 5 - Availability of PMS Documentation for GDA Assessment

Lifecycle Phase	PMS
Design Requirements	A
System Definition	A*
Design	B
Implementation	B
Test	B
Installation	C

Note – A* denotes some documents will be missing.

26. I consider the level of detail acceptable as it aligns with that expected for a PCSR at the GDA stage and recognises that the PMS using the Common Q platform will need to be developed to meet the specific needs of the UK **AP1000** project.

3 REQUESTING PARTY'S SAFETY CASE

27. Westinghouse's safety case for the PMS is based on the presentation of a BSC along with supporting references that demonstrate that the PMS satisfies the GDA issue. The Westinghouse safety case for GDA Issue GI-AP1000-CI-08, PMS Adequacy of Safety Case is documented in:

- UKP-PMS-GLR-001 Rev 2, United Kingdom AP1000® Protection and Safety Monitoring System Safety Case Basis, December 2016 (Ref. 2);
- Key references to the BSC including those referenced in the Westinghouse resolution plan (Ref. 3)
  - UKP-PMS-GL-010 Rev 2, United Kingdom AP1000 PMS Safety Assessment Principle Evaluation, December 2016 (Ref. 8)
  - UKP-PMS-GL-012 Rev 1, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Protection and Safety Monitoring System, December 2016 (Ref. 9)
  - UKP-PMS-GL-002 Rev 2, United Kingdom AP1000 IEC 60880 Compliance Matrix for the Protection and Safety Monitoring System, July 2016 (Ref. 10)
  - UKP-PMS-GLR-007 Rev 1, United Kingdom AP1000 IEC 60987 Compliance Matrix for the Protection and Safety Monitoring System, July 2016 (Ref. 11)
  - UKP-PMS-GL-005 Rev 1, United Kingdom AP1000 Protection and Safety Monitoring System AC160 Suitability Analysis, December 2016 (Ref. 12)
  - WEG-AR-00579-GEN Rev 00, IEC 60987 Compliance Matrix for the AC160 Product HW as integral part of the Protection and Safety Monitoring System, July 2016 (Ref. 13)
  - GBRA095803 Rev D, O1-MOD – Qualification Final Quality Assessment and Justification Report – Addendum, December 2016 (Ref. 14)

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-08, PMS ADEQUACY OF SAFETY CASE

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

4.1 Scope of Assessment Undertaken

29. The scope of my assessment covered the Westinghouse submissions identified in the GDA issue resolution plan (Ref. 3). This included the PMS BSC (Ref. 2), the PMS SAP CAE (Ref. 8), the PMS IEC 61513 CAE (Ref. 9), the PMS IEC 60880 Compliance Matrix (Ref. 10), the PMS IEC 60987 Compliance Matrix (Ref. 11), the AC160 Suitability Analysis (Ref. 12), the AC160 IEC 60987 Compliance Matrix (Ref. 13) and the Final Quality Assessment and Justification Report - Addendum (FQAJ-A) (Ref. 14). I also sampled supporting documents referenced from these main submissions.

30. Westinghouse’s submissions in this topic area may address some of the GDA Step 4 assessment findings (Ref. 7). However, it is the responsibility of the licensee to demonstrate closure of all assessment findings including those generated at Step 4 of the GDA. The assessment of the closure of Step 4 assessment findings is therefore outside the scope of this report. The licensee should consider the Westinghouse submissions in this area when making the case for closure of the assessment findings.

4.2 Assessment

31. My assessment of Westinghouse’s submissions provided in response to GDA Issue GI-AP1000-CI-08, PMS Adequacy of Safety Case is discussed below. ONR reviewed the submissions provided in response to GI-AP1000-CI-08 in order to determine whether GDA Issue Actions GI-AP1000-CI-08.A1 and GI-AP1000-CI-08.A2 had been addressed. Requests for clarification were raised by RQs. As appropriate, Westinghouse revised the submitted documents to address the points raised in the RQs. The description of the scope of work performed by the TSC in support of my assessment and the TOs arising from its work are contained in a TSC report (Ref. 15).

32. The PMS is the Class 1 primary C&I safety system for the **AP1000** plant and, as such, it principally fulfils Category A reactor trip and engineered safety feature (ESF) actuation functions. The PMS also provides Class 1 displays and controls of key plant parameters and equipment in the main control room and the remote shutdown room. The reliability claim for the PMS is 1E-3 probability of failure on demand (pfd).

33. The PMS comprises two main platforms, the Common Q platform and the Component Interface Module (CIM), supplemented by a spurious actuation blocking device. The Common Q platform principally includes Asea Brown Boveri (ABB) AC160 Programmable Logic Controllers and a computer-based Flat Panel Display System (FPDS). The Basis of Safety Case (Ref. 2) provides a full description of the platforms and architecture of the PMS.

34. The CIM is a field programmable gate array (FPGA) based module that provides the PMS interface to the field components (e.g. valves, circuit breakers). The CIM 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. The detailed safety justification for the CIM is the subject of GDA Issue GI-AP1000-CI-09 and is assessed in a dedicated ONR assessment report (Ref. 18).

35. The blocking device is based on simple non-programmable hardware. It prevents the spurious actuation of a number of PMS ESF functions by providing an independent permissive signal, which allows actuations to occur only if plant conditions are

appropriate. The detailed safety justification for the blocking device is the subject of GDA Issue GI-AP1000-CI-04 and is assessed in a dedicated ONR assessment report (Ref. 19).

36. GDA Issue GI-AP1000-CI-08 had two associated actions: GI-AP1000-CI-08.A1 required access to all safety justification documentation for the PMS in the UK, and GI-AP1000-CI-08.A2 required the provision of a BSC for the PMS. I discuss my assessment of Westinghouse's response to these actions below.

4.2.1 GDA Issue Action GI-AP1000-CI-08.A1 – Access to Detailed Evidence in the UK

37. GI-AP1000-CI-08.A1 required Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the BSC for the PMS application and the AC160 platform. In response to this action Westinghouse made all PMS documents available to ONR in the UK. Westinghouse submitted the formal documents identified in the resolution plan as they became available in accordance with its rescheduled submission programme. In addition, the company submitted further supporting documents to ONR in response to RQs. I also reviewed commercially sensitive supplier evidence at the ABB Stonehouse facility in the UK (see Ref. 34). I am satisfied that, as a result of the provision of access to documents in the UK, Westinghouse has satisfactorily addressed GDA Issue Action GI-AP1000-CI-08.A1.

4.2.2 GDA Issue Action GI-AP1000-CI-08.A2 – Provision of a BSC for the PMS

38. GI-AP1000-CI-08.A2 required Westinghouse to provide a BSC for the PMS that takes into account ONR expectations for such a document. My review of the submissions provided in response to this GDA issue action is provided below.

39. I undertook my review of the PMS BSC (Ref. 2) to:

- confirm that the submission had adequately addressed the topics and elements of a BSC as outlined in the GDA issue and ONR GDA Issues Closure Guidance Document (Ref. 16) (note that I supplied Ref. 16 to Westinghouse as additional guidance on the content of BSCs; in the letter supplying this guidance (Ref. 17) I explained that it is the Requesting Party's (RP's) responsibility to consider and provide a comprehensive safety submission addressing each of the GDA issues);
- check the adequacy of the CAE for the PMS lifecycle (e.g. that Westinghouse had adequately addressed the requirements of IEC 61513 Clause 6 "system safety life cycle");
- determine if Westinghouse had addressed the TOs identified for further guidance in the GDA issue;
- confirm that CAE trails were adequate, including links to supporting documents; and
- identify any technical concerns with the document.

40. I found that the PMS BSC (Ref. 2) addressed the following topics:

- The high-level claims on the PMS, the relevant industry standards, and an overview of the supporting documentation that contains production excellence and independent confidence-building evidence (in accordance with ONR technical assessment guide NS-TAST-GD-046, Ref. 6).

- The context of the PMS BSC in relation to the PCSR, other BSCs, and the PMS 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 captures how and when Westinghouse will implement the compensating measures identified in its SAPs and standards compliance assessments (e.g. 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 PMS 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 PMS.
- The ALARP case for the PMS.
- How Westinghouse has addressed the findings from previous assessments of the PMS (including those by other regulators).
- The approach taken to address GDA Step 4 TOs.

41. The detail of the CAE for conformance to the SAPs and standards is not contained in the BSC but is provided in separate documents (i.e. Refs 8, 9, 10, 11 and 13). My assessment of these documents may be found below.

42. The detailed findings from my assessment of the PMS BSC (Ref. 2) and its key supporting documents (Refs 8, 9, 10, 11 and 13) may be found in Ref. 15. In summary, I found that the structure and content of these submissions broadly met my expectations in terms of BSC topics and elements as outlined in the GDA issue and supporting guidance.

43. I noted that the safety plan in Section 4 of Ref. 2 describes how the UK PMS is derived from the **AP1000** standard plant design. The plan describes how a number of design changes have occurred as a result of the GDA process and that, as a result, the PMS safety lifecycle phases will be repeated post GDA to incorporate the UK **AP1000** design requirements.

44. In accordance with the guidance in Ref. 16, the safety plan in Ref. 2 provides a list of future PMS safety life cycle activities and PMS safety demonstrations. Ref. 2 also includes a schedule for the complete lifecycle of the development of the PMS for the **UK AP1000** plant, from concept / planning to operation and maintenance. The deliverables affected by the design changes are identified for each phase of the development, with indicative timescales for their delivery based on the start of an engineering, procurement and construction (EPC) contract. The commitment is made in Section 4 to maintain the BSC post GDA as the lifecycle phases are completed.

45. While I found the topics and elements of the BSC and supporting documents to be broadly acceptable, in my review of Ref. 2 I raised a number of queries with Westinghouse, both through RQs and at level 4 meetings. The detailed content of these queries, and the assessment of the Westinghouse responses, may be found in Ref. 15 and Ref. 28. The most significant of the queries covered topics including:

- PMS reliability

- functions implemented in a non-2oo4 configuration
- metrication
- statistical testing
- programmable complex electronic components (PCECS)
- PMS BSC supporting documents

46. I discuss my assessment of these topics below.

4.2.2.1 PMS Reliability

47. A key component of the safety justification of a safety system such as the PMS is a demonstration that the reliability claim for the functions it fulfils has been achieved (see NS-TAST-GD-003). In support of my assessment of the PMS BSC (Ref. 2), I sampled the approach taken to the analysis of hardware reliability for the PMS and the results of that analysis.

48. The Westinghouse reliability claim for the PMS is 1E-3 pfd. In support of this claim, the PMS BSC (Ref. 2) and supporting document AP1000 Protection and Safety Monitoring System Reliability Analysis (Ref. 20) describe the method for and the results of a quantitative hardware reliability analysis undertaken on the system.

49. I reviewed Refs 2 and 20 and determined that the method uses reliability block diagrams supported by a commercially available tool (217Plus™) for the derivation of component failure rate values. I found that the calculated values are conservative since all failures are considered rather than just dangerous failures. Following consultation with the ONR PSA inspector I concluded that the overall hardware reliability analysis method was appropriate.

50. I found that the results of the analysis were expressed in units of failures per year rather than probability of failure on demand. I also found that common cause failures (CCF) within the PMS had not been addressed. Consequently, I raised RQ-AP1000-1737 seeking clarification on these points. In particular, I requested an analysis illustrating the worst-case reliability examples for each of the voting architectures utilised by the PMS (e.g. 1-out-of-2 (1oo2), 2oo3, 2oo4). This analysis was to include all aspects of the system including the CIM and the spurious actuation blocking device.

51. Westinghouse acknowledged in its response to RQ-AP1000-1737, and subsequently in a revision to the PMS BSC (Ref. 2), that the units identified in Section 1.4 of the reliability analysis document (Ref. 20) were incorrectly expressed as failures per year rather than pfd. Westinghouse undertook to revise the document when the analysis of the UK **AP1000** detailed design is undertaken post GDA. Westinghouse also provided the results of its analysis of different voting architectures; this illustrated that the hardware reliability for Category A functions implemented in a 2oo4 configuration in the PMS when accounting for CCF is 3E-4 pfd, thereby meeting the claim of 1E-3 pfd.

52. I noted that, while addressing CCF, Westinghouse had used figures for beta factors based on the reactor protection system for the Swedish Ringhals reactor plant. The reactor protection system for this plant uses Westinghouse technology; however the analysis was undertaken in 2005 and may not adequately reflect the UK **AP1000** specific PMS hardware design. I also noted that figures for test intervals are based on the standard plant arrangements. The beta factor and test interval figures require review and justification once the detailed design of the **UK AP1000** plant is undertaken

and the licensee determines its plant-specific examination, inspection, maintenance and test arrangements. I have captured this expectation in Assessment Finding CP-AF-AP1000-CI-011 below.

53. The overall reliability value for the PMS is the sum of the hardware and software values (see Clause A3.7 of NS-TAST-GD-046). The justification that the PMS meets the 1E-3 claim with regard to software reliability is provided in documents including the standards compliance matrices (Refs 9, 10, 12 and 14). My assessment of the adequacy of these safety justifications is discussed in Section 4.2.2.6 of this report. The findings from these assessments, as detailed in Ref. 15 and summarised in this report, will need to be addressed by the licensee to complete the overall reliability analysis for the UK **AP1000** PMS. This requirement is captured in Assessment Finding CP-AF-AP1000-CI-011 below.

54. I noted that an apparent discrepancy arose regarding the reliability figures claimed for the PMS in the C&I documentation when compared with those figures used in the overall plant PSA. The ONR PSA assessment report (Ref. 21) discusses the sensitivity of the risks to the reliability of the PMS. It concludes that when using the PMS reliability figures derived from the C&I analysis (1E-3 pfd) in the derivation of the core damage frequency, the risk remains well below the ONR Target 8 Basic Safety Level.

55. Following assessment of Westinghouse's submissions associated with the hardware reliability analysis of the PMS, I am content that the method used and the results achieved are adequate. I have raised the following assessment finding to capture those matters arising from my assessment that need to be addressed during implementation of the PMS.

> GDA Assessment Finding: **CP-AF-AP1000-CI-011** – The licensee shall justify the reliability of the detailed PMS design in the safety case including but not limited to:
>
> - provide a probability of failure on demand figure for each individual safety function which includes all sources of random, common mode and systematic failures;
> - provide a justification for the beta factors and test intervals used in the reliability analysis that is based on the UK **AP1000** detailed design and implementation; and
> - update the overall UK **AP1000** plant PSA, as necessary, to reflect the as-designed reliability calculations.

4.2.2.2 Functions Implemented in a Non-2oo4 Configuration

56. The ONR C&I Step 4 assessment report (Ref. 7) describes how the PMS four-fold 2oo4 voted divisional architecture with dual redundancy within the divisions is an effective approach consistent with current good practice for protection systems on modern nuclear power plants.

57. The report explains that, should it be necessary to withdraw a division from service (e.g. for maintenance), a veto (bypass) is applied and the remaining three divisions revert to 2oo3 voting logic. This arrangement is also resilient to equipment failure within a division. Should a division be lost (e.g. because of equipment failure within the division), the voting logic of the other three divisions becomes 1oo3. The application of a veto (bypass) to stop the trip demand from the failed division changes the voting

logic to 2oo3. This overall approach therefore affords conformance with ONR SAP EDR.4 – Single Failure Criterion.

58. The Step 4 report also identifies that in some cases PMS functions are provided using fewer than four divisions. Consequently, Step 4 Assessment Finding AF-AP1000-CI-024 was raised stating:

> The licensee shall demonstrate that the differences of functional coverage across the PMS divisions do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a division, or any division is taken out of service for maintenance. For further guidance see T16.TO2.07 in Annex 6.

59. 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 any case for closure of the assessment findings.

60. I found in my review of the ALARP section of the PMS BSC (Ref. 2) that eight safety functions have reduced levels of redundancy (based on historical decisions on their perceived significance) and that in some instances this reduced level of redundancy challenges the single failure criterion as defined in SAP EDR.4.

61. The BSC describes how each of these safety functions has now been categorised in accordance with IEC 61226, assessed for conformance against the single failure criterion and related SAPs, and assessed for their contribution to risk reduction. Westinghouse then considered the relative benefits or otherwise of modifying their configuration based on these assessments.

62. The outcome of this analysis was a reduction in the safety category of a number of the functions (i.e. from Category A to Category B or C), and a series of recommendations to modify the configuration of the voting logic of three of the functions as follows:

- Voting logic for the Automatic Depressurisation System Stage 4 and the In-containment Refuelling Water Storage Tank (IRWST) actuation based on hot-leg level to be made 2oo4 instead of the current 1oo2.
- IRWST level based actuation of spent fuel cooling system isolation to be made 1oo3 instead of 1oo2.
- A second actuation based on low hot-leg level (the Category C function Chemical and Volume Control System letdown isolation) to be made 2oo4 instead of 1oo2.

63. I found that these recommendations have been carried forward to the BSC safety plan. I have raised the following assessment finding, to be read in conjunction with Step 4 Assessment Finding AF-AP1000-CI-024, for the licensee to justify the adequacy of the PMS architecture while considering the re-categorisation of safety functions and the recommended modifications during detailed design of the PMS post GDA:

> GDA Assessment Finding: **CP-AF-AP1000-CI-012** – The licensee shall justify the final PMS architecture and detailed design taking into account the re-categorisation of safety functions and the modifications recommended in the BSC safety plan (Ref. 2). For guidance on this assessment finding see also Step 4 Assessment Finding AF-AP1000-CI-024.

4.2.2.3 Metrication

64. The standard **AP1000** design is based on the use of imperial rather than metric units; this was identified as a cross-cutting issue in GDA Step 4 and the ONR C&I Step 4 report discusses it (Ref. 7).

65. As part of the close-out of mechanical GDA Issue GI-AP1000-ME02, Metrication of Mechanical Equipment and Civil Structural Steelwork Connections, Westinghouse submitted AP1000® Plant Metrication Strategy and ALARP Assessment for the United Kingdom (Ref. 23). I reviewed the C&I aspects of this document with the ONR mechanical engineering inspector.

66. Following my review, I raised a number of queries on the multidisciplinary RQ-AP1000-1346, as issued to Westinghouse by the ONR mechanical engineering inspector. In summary, I requested clarification regarding how Westinghouse proposed to mitigate the risk of systematic errors being built into software in the C&I systems when implementing a standard imperial-based design on a UK metric plant.

67. In response to the PMS-related aspects of RQ-AP1000-1346 and following discussions at a level 4 meeting (Ref. 24), Westinghouse included a metrication section in the PMS BSC (Ref. 2).

68. I reviewed the metrication section of the BSC and found that it describes how data associated with set-points and engineering unit conversion is captured in a database and subsequently used in the design and implementation of the PMS software. I found that the section also describes how analogue sensor inputs to the PMS are converted to engineering units by a EUCONVRT software module using data derived from the aforementioned database. I also found that a number of software algorithms within the PMS only operate with imperial units. For such modules, a further UTCONVRT software module is used to convert sensor inputs and addressable constants to imperial units before their processing, and to convert the units back to metric following processing. The UTCONVRT functionality is enabled and disabled through a flag in the software. The BSC also provides a high-level description of the verification and validation activities associated with all of the software mentioned above.

69. I am content that the description of the development of the engineering unit conversion software provided in the PMS BSC is adequate for GDA. However, given the critical nature of this software in fulfilling safety functions across the PMS, I have raised the following assessment finding to ensure that the licensee provides a fully detailed safety justification of the adequacy of its design, implementation, verification and validation in order that any potential systematic faults therein are not propagated to the runtime environment of the PMS.

> GDA Assessment Finding: **CP-AF-AP1000-CI-013** – The licensee shall justify the final as-built PMS software associated with the derivation and conversion of set-points and engineering units.

4.2.2.4 Statistical Testing

70. When discussing software reliability, NS-TAST-GD-046 states that numerical claims are enhanced by the application of statistical testing techniques. Westinghouse proposed to use such a technique as an independent confidence-building measure for the PMS.

71. Westinghouse described the approach it intends to take for statistical testing of the PMS in documents produced on its behalf by AMEC Foster Wheeler – AP1000 Statistical Testing Plan Approach (Ref. 26) and UK AP1000 PMS Statistical Testing - Test Plan (Ref. 27). The detail of my assessment of Refs 26 and 27 may be found in a note for the record (Ref. 28). An overview is below.

72. I found that Ref. 26 provides a high-level overview of the steps required to produce an acceptable statistical testing programme while Ref. 27 contains the required information to perform the statistical tests. I raised a series of queries seeking clarification on these documents on RQ-AP1000-1408, RQ-AP1000-1555, RQ-AP1000 1673 and RQ-AP1000-1689 as the development of the approach progressed. I have outlined my principal lines of inquiry below.

73. Westinghouse initially proposed to apply 5000 tests to the one of the four PMS divisions that contains the same complete set of hardware as on all of the other divisions, thereby providing a demonstration of better than 1E-3 pfd with a 99% confidence level for that division. Westinghouse planned to perform 230 tests on each of the other three divisions. I noted that the configuration of the four divisions of the PMS is not identical and queried the statistical basis for the number of tests on the three divisions. Westinghouse responded by committing to perform 700 tests on each of these three divisions, thereby providing a demonstration of 1E-3 pfd with a 50% confidence level for each of those divisions. I judge this to be a reasonable approach as it provides a confidence level consistent with PSA expectations for reliability data.

74. I queried the reasonable practicability of repeating a complete set of statistical tests following software modifications as it may be considered that a modification produces a new software version. Westinghouse responded with an update to Ref. 26, which states:

    The nature, potential impact and imperativeness of any software modifications would require assessing on a case by case basis, by the licensee and an appropriate level and type of regression testing substantiate(d) and performed (e.g. stati(sti)cally testing, targeted testing and black box functional test). As it is expected that a suit(e) of 7100 statistical test could be completed in a little over four weeks, the maintenance burden could be managed such that software modifications are grouped and implemented during a planned plant outage, and a full suite of statistical tests performed following each batch of updates (software modification).

75. This represents an adequate response to my query but it places a responsibility on the licensee to make allowance in its management systems to determine the reasonable practicability of repeating a full suite of statistical tests following software modifications. I have therefore captured this expectation in Assessment Finding CP-AF-AP1000-CI-014 below.

76. I requested clarification regarding the factors that will be considered in determining the appropriate reset time between individual tests (e.g. presence of timers, counters, time constants/filters and other memory-dependent features). In response Westinghouse stated that the use of resets will be investigated further during detailed design of the test platform. The need to confirm this important aspect of the test approach (i.e. appropriateness of the reset period) is therefore included in Assessment Finding CP-AF-AP1000-CI-014 below.

77. I requested Westinghouse to clarify the method for generating each individual test including the approach taken to linearisation of the probability distributions and what noise factors are to be applied. Westinghouse provided clarification on the approach to be taken to development of the tests, including the factors mentioned, but stated that the detailed definition of these requires input from the system owner / operator (licensee), transient specialists and process engineers. Assessment Finding CP-AF-

AP1000-CI-014 below includes the requirement to define and justify these detailed aspects of the test design.

78. In summary, I judge that through Refs 26 and 27 Westinghouse has presented a satisfactory position in relation to statistical testing of the PMS and has demonstrated a reasonable understanding of the topic area. The licensee will need to ensure that the statistical testing programme for the PMS is fully implemented during site licensing and that the outstanding points identified in Assessment Finding CP-AF-AP1000-CI-014 below are addressed.

> GDA Assessment Finding: **CP-AF-AP1000-CI-014** – The licensee shall implement a statistical test programme for the PMS that includes but is not limited to:
>
> - regression testing following software modifications;
> - definition and justification of linearisation curves and noise factors; and
> - definition and justification of test reset characteristics including reset periods.
>
> For further guidance on this assessment finding, see Ref. 28.

4.2.2.5 Programmable Complex Electronic Components

79. In addition to microprocessor-based modules, the PMS also contains a number of PCECs such as FPGAs. The ONR GDA Step 4 C&I assessment report for the Westinghouse **AP1000** reactor (Ref. 7) states the following regarding PCECs in the PMS:

> The AC 160 platform uses a number of PCECs, for example, in the interfaces to the back plane, high speed link (HSL) and AF100 bus. The correct operation of these devices is crucial to ensure delivery of the safety functions and determinism of the system. My assessment determined that the development processes used for the PCECs do not align with my expectations for a demonstration of production excellence (e.g. as judged against the expectations set down in the PCEC checklist). Compensatory measures are needed to address the production excellence gaps. A justification of the adequacy of the compensatory measures taken (e.g. as compared with the expectations in the PCEC checklist (Ref. 64)) is required. A safety demonstration will be needed for each PCEC development process.

80. Step 4 Assessment Finding AF-AP1000-CI-010 was raised to ensure that the licensee addresses these findings:

> The licensee shall produce a safety justification for each Programmable Complex Electronic Component (PCECs) used in all Systems Important to Safety. The licensee shall identify any deviations (i.e. gaps) from production excellence (as judged against an agreed standard) and demonstrate how the compensatory measures have adequately closed the gaps. This shall include demonstrating how test scripts were derived (e.g. from the requirements) and completion of the PCEC checklist. For further guidance see T15.TO2.01 b and d, T15.TO2.08, T15.TO2.27 and T15.TO2.39 a, b and c in Annex 5.

81. 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.

82. Westinghouse claim in Table 4.7-1 of the PMS BSC (Ref. 2) that AF-AP1000-CI-010 has been completed as part of GDA. While the closure of assessment findings is a matter for the licensee, I found in my assessment of the BSC that Table 6.1-4 in Section 6.1.10.1.4 summarises the production excellence, compensating measures and independent confidence-building measures for the 22 PCEC types within the AC160 (note that the PMS will contain multiple instances of each type).

83. Westinghouse describes in Section 6.1.10.1.4 the heritage of the PMS PCECs and acknowledges that:

> At the time of their development there was not a nuclear industry standard for a safety life cycle for these devices. As a result, there is scant evidence of a safety life cycle for the devices and therefore none of the PCECs have a complete demonstration of a safety life cycle.

84. In my review of this section I found a lack of visibility of any assessment of the development lifecycles of the PCECs against a good practice standard such as IEC 62566. I found that that the compensating measures identified for each of the PCECs were not supported by a justification as to why they address the gaps in the production excellence demonstration. I also found that independent confidence-building measures were not supported by a justification of their adequacy, nor of the independence of the personnel implementing them.

85. I found that, in the PMS BSC (Ref. 2) safety plan (Section 4), Westinghouse commits to the qualification of PCECs in the AC160 considering IEC 62566, to functional analysis of the source code and to black box testing of a number of the PCECs. The safety plan also commits to the development of a plan for the qualification of the PCECs within the FPDS.

86. I conclude that Step 4 Assessment Finding AF-AP1000-CI-010 regarding PCECs is yet to be fully addressed. In addition to those concerns identified at Step 4, the licensee should implement the PMS BSC safety plan (Ref. 2) and address the findings from this assessment when doing so. I have captured the requirement for the licensee to address these additional issues in Assessment Finding CP-AF-AP1000-CI-018 in Section 4.2.2.7 below.

4.2.2.6 PMS BSC Supporting Documents

87. In support of my assessment of the PMS BSC (Ref. 2) I reviewed the following key supporting documents and sampled their references:

- PMS Safety Assessment Principles Evaluation (Ref. 8)
- IEC 61513 CAE for the PMS (Ref. 9)
- IEC 60880 Compliance Matrix for the PMS (Ref. 10)
- IEC 60987 Compliance Matrix for the PMS (Ref. 11)
- IEC 60987 Compliance Matrix for the AC160 Product Hardware (Ref. 13)
- PMS AC160 Suitability Analysis (Ref. 12)
- O1-MOD – Qualification Final Quality Assessment and Justification Report – Addendum (Ref. 14)

- Proprietary ABB documents supporting the AC160 Suitability Analysis (Ref. 12) and the FQAJ Addendum (Ref. 14) were inspected at the ABB Stonehouse facility

88. I discuss my assessment of these key supporting documents and their references below. The detail of the approach to, and findings from, my assessment may be found in Refs 15 and 34.

89. I found in my review of all of the standards compliance documents (Refs 9, 10, 11 and 13) that the treatment of the requirements of the standards varies. I found that that only "shall" statements are provided with a full CAE trail with gaps and compensating measures identified where necessary; "may" and "should" statements are either not addressed or do not have gaps or compensating measures identified. I found a similar approach across all of the standards conformance demonstrations for all of the C&I systems (i.e. PMS, CIM, Blocker, Diverse Actuation System, PLS, Data Display and Processing System).

90. I raised generic RQ-AP1000-1707, requesting that Westinghouse fully addresses all "may" and "should" clauses and sub-clauses in standards conformance assessments, or, if this is not considered reasonably practicable, 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.

91. In its 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.

92. 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.

93. The detailed findings from my review of the standards compliance documents (Refs 9, 10, 11 and 13) are not captured within AF-AP1000-CI-005. I have therefore raised the following assessment finding, 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 PMS. 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-015** – The licensee shall address all "should" and "may" statements in all standards conformance assessments for the PMS.
>
> For further guidance on this assessment finding see also Step 4 Assessment Finding AF-AP1000-CI-05 and CI-08-TO2-2.2.2.4.6-2 in Ref. 15.

PMS Safety Assessment Principles Evaluation

94. The PMS Safety Assessment Principle Evaluation document (Ref. 8) determines conformance of the PMS to those SAPs that Westinghouse considers to be appropriate for a Class 1 safety system. It provides a demonstration that the SAPs are met through a CAE trail for each SAP.

95. I reviewed Ref. 8 to confirm adequate coverage of those SAPs applicable to a Class 1 safety system such as the PMS. I also sampled in detail (Ref. 15) the CAE trails associated with SAPs ESS.27, ESS.21, ESS.22, EDR.1 and EQU.1. Following my review I raised a number of queries in RQ-AP1000-1668, in particular in relation to the demonstration of adequate production excellence and independent confidence-building measures associated with ESS.27.

96. I found that Westinghouse's response to RQ-AP1000-1668 adequately addressed my queries and that Ref. 8 met my expectations in terms of the coverage of SAPs, with clear CAE trails provided. I found instances where the CAE trails identified gaps and compensating measures against a number of the SAPs. These were summarised in Table 3.1-1 of the document and were taken forward to the PMS BSC (Ref. 2) safety plan, to be addressed in the design phase post GDA.

IEC 61513 Claims, Arguments and Evidence for the PMS

97. The purpose of the United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence document (Ref. 9) is to demonstrate the extent of conformance of the PMS with IEC 61513. The document provides the CAE of the PMS development activities and the Westinghouse documentation against the applicable IEC 61513 requirements in a tabular format. In this respect the document extends the high-level claims based on the requirements of IEC 61513 captured in Section 5 of Ref. 2.

98. I reviewed Ref. 9 and raised a number of queries on RQ-AP1000-1732. In particular, I found that the "should" and "may" IEC 61513 clauses had not been addressed, as described earlier in this report. Westinghouse's commitment in its response to RQ-AP1000-1707 to update all of the C&I standards conformance assessments in this regard (as captured in Assessment Finding CP-AF-AP1000-CI-015) addresses this issue for Ref. 9.

99. I also found instances where the CAE trails identified gaps and compensating measures against a number of the clauses of IEC 61513. These were summarised in Appendix B of the document and were taken forward to the PMS BSC (Ref. 2) safety plan.

100. I assessed Westinghouse's response to RQ-AP1000-1732 and found that my queries had largely been addressed through an update to Ref. 9. A small number of minor points remain, which have been captured in TO CI-08-TO2-2.2.2.8.4-1 in Ref. 15, to be addressed in the design phase of the PMS development lifecycle post GDA (see Assessment Finding CP-AF-AP1000-CI-018 below).

IEC 60880 Compliance Matrix

101. I reviewed the United Kingdom AP1000 IEC 60880 Compliance Matrix for the Protection and Safety Monitoring System (Ref. 10), the purpose of which is to demonstrate the extent of conformance to IEC 60880 for the PMS application software. Westinghouse used a tabular approach to this demonstration that provides CAE trails for decomposed requirements of the standard using the Dynamic Object-Oriented Requirements System (DOORS®) tool.

102. In my review of Ref. 10 I observed a number of aspects of the conformance matrix that required clarification. These were initially identified on RQ-AP1000-1527, which was then supplemented by RQ-AP1000-1587.

103. The responses to the RQs largely provided the requested clarifications. However, I identified in the response to RQ-AP1000-1527 some ambiguity concerning the operating system to be used for the FPDS. I subsequently raised RQ-AP1000-1778, where I requested further clarity regarding the use of the standard plant design QNX™ operating system on the UK **AP1000** plant.

104. Westinghouse explained in its response to RQ-AP1000-1778 that the QNX™ operating system was developed without a safety lifecycle and was commercially dedicated, relying heavily on its operating history. Westinghouse stated that it has been determined not to meet the criteria of IEC 60880 and would not be used for the FPDS on the UK **AP1000** plant. Westinghouse described the approach to be taken post GDA: an optioneering study for the selection of an alternative operating system that would subsequently undergo a commercial dedication program in order to demonstrate adequate conformance with IEC 60880.

105. I requested further clarification at a level 4 meeting regarding the feasibility of identifying an operating system that would fulfil the PMS functional and non-functional requirements and would meet ONR expectations for a Class 1 system (see Ref. 25).

106. Westinghouse responded with a revision to Ref. 2, which described in the safety plan (Section 4.3.2.3) a preliminary optioneering study that it undertook following my query. This preliminary study identified two candidate commercially available operating systems that have previously received certification to a number of international safety standards, including IEC 61508 to Safety Integrity Level 3. Westinghouse committed in the safety plan to complete the optioneering study and qualify the selected operating system to IEC 60880 before the completion of the detailed design of the FPDS post GDA.

107. In addition to completing the demonstration that the selected operating system adequately conforms with IEC 60880 (i.e. the production excellence case), Westinghouse identified the following independent confidence-building measures to be applied to the operating system as the development of the FPDS progresses post GDA:

- UK **AP1000** channel integration test and system integration test
- tool based static semantic analysis (if source code is available)
- statistical testing
- focused operating system dynamic testing
- examination, inspection, maintenance records review
- proof test records review

- independent review of tools
- Functional Safety Assessment (against PMS requirements)

108. I am satisfied that the approach taken for the identification and justification of the operating system for the FPDS is adequate given the early stage of development of the FPDS. I have raised the following assessment finding to capture those matters that need to be addressed during the development of the FPDS post GDA:

> GDA Assessment Finding: **CP-AF-AP1000-CI-016** – The licensee shall justify that the selected operating system for use with the Flat Panel Display System (FPDS) meets Class 1 requirements.
>
> For further guidance on the completion of the FPDS operating system justification see Technical Observation CI-08-TO2-2.2.2.4.6-4 in Ref. 15.

IEC 60987 Compliance Matrix for the PMS

109. I assessed the document United Kingdom AP1000 IEC 60987 Compliance Matrix for the Protection and Safety Monitoring System (Ref. 11), the purpose of which is to demonstrate the extent of compliance with IEC 60987 for the PMS hardware design. The document demonstrates the extent of compliance by providing a compliance matrix that correlates the IEC 60987 requirements to the applicable evidence in the documentation associated with the Westinghouse UK **AP1000** design.

110. I noted that this document addresses compliance with IEC 60987 for the PMS application hardware design only. The evaluation of the ABB AC160 product hardware against this standard is contained in a separate document (Ref. 13; see assessment below).

111. I reviewed Ref. 11 and found that, as with the other Westinghouse standards conformance submissions, it does not fully address the “should” and “may” clauses of IEC 60987. Westinghouse’s commitment in its response to RQ-AP1000-1707 to update all of the C&I standards conformance assessments in this regard (as captured in Assessment Finding CP-AF-AP1000-CI-015) addresses this issue for Ref. 11.

112. Where Westinghouse found a partial compliance or non-compliance against a “shall” statement from the standard, a compensating measure was identified. Westinghouse initially captured these compensating measures in Appendix B of Ref. 11 and subsequently brought them forward to Table 4.1-2 of the PMS BSC safety plan (Ref. 2). I noted that Appendix B does not identify the need to complete an IEC 60987 compliance assessment for the FPDS. I subsequently reviewed the PMS BSC safety plan where this requirement is clearly stated in Section 4.3.2.6, thereby addressing this concern.

113. I confirmed that all other outstanding compensating measures identified in Appendix B of Ref. 11 were brought forward to the PMS BSC (Ref. 2) safety plan where the timescale for their implementation is identified.

114. I raised RQ-AP1000-1552 and subsequently RQ-AP1000-1671 to capture a number of further queries arising from my review. The Westinghouse responses to the RQs, along with an update to the compliance matrix, provided satisfactory resolution of the points raised.

IEC 60987 Compliance Matrix for the AC160 Product Hardware

115. The purpose of the document IEC 60987 Compliance Matrix for the AC160 Product Hardware as integral part of the Protection and Safety Monitoring System (Ref. 13) is to demonstrate the extent of compliance with all product-related aspects of IEC 60987 for the AC160 product hardware used for the PMS. In this respect Ref. 13 may be considered to be an extension of Ref. 11 that addresses those aspects of IEC 60987 related to the system hardware design (see assessment above).

116. I reviewed Ref. 13 on a sampling basis to ensure that correct traceability exists between the IEC 60987 compliance matrix for the AC160 product and the IEC 60987 compliance matrix for the PMS hardware design (Ref. 11). I also considered in particular the statements of partial and non-compliance with the standard in order to determine whether they had been managed appropriately.

117. I found from my review that, as with other standards compliance assessments, the treatment of different requirement types varies (i.e. “should” and “may” statements from the standard did not have compensating measures identified for partial or non-compliance). The Westinghouse commitment to update all of the standards compliance assessments in response to RQ-AP1000-1707 addresses this concern for Ref. 13.

118. Where partial compliance or non-compliance was found against a “shall” statement from the standard, a compensating measure was identified. These compensating measures were initially captured in Table 5-1 of Ref. 13 and were subsequently brought forward to Table 4.3.1.2-1 of the PMS BSC safety plan (Ref. 2).

119. In my traceability review, I found a small number of minor anomalies between Ref. 13, Ref. 11 and the PMS BSC safety plan (Ref. 2). These anomalies are captured in detail in TO GI-08-TO2-2.2.2.2.4-1 in Ref. 15. I am satisfied that the licensee may deal with these minor anomalies during the detailed design of the PMS and as such have captured the TO under Assessment Finding CP-AF-AP1000-CI-018.

AC160 Suitability Analysis

120. The purpose of the United Kingdom AP1000 PMS AC160 Suitability Analysis (Ref. 12) is to present the Westinghouse evaluation of the ability of the ABB AC160 product to satisfy the requirements of the **AP1000** PMS.

121. I reviewed Ref. 12 and selected references on a sampling basis to determine, for example, the adequacy of the approach taken to compilation of requirements, whether the use of the reference plant requirements is appropriate for the UK **AP1000** reactor and whether the CAE trails are adequate. Ref. 15 contains a full description of the scope of the review.

122. Following my review, I raised a number of queries on RQ-AP1000-1716. These queries addressed topics associated with the detail of the approach taken to collation of requirements for the AC160 and the completeness of the requirements identified.

123. Westinghouse provided a response to RQ-AP1000-1716 albeit that a number of detailed points remained to be addressed. These are captured under TO CI-08-TO2-2.2.3.4.4-1 in Ref. 15. I am satisfied that the licensee may deal with these detailed points during the requirements phase of the UK **AP1000** PMS development process and as such have captured the TO under Assessment Finding CP-AF-AP1000-CI-018.

124. I noted through my review that Ref. 12 references the AP1000 PMS Requirements Traceability Matrix (Ref. 29). Ref. 29 is developed using the DOORS® tool and

captures in a tabular fashion the traceability of requirements to PMS design documents from sources such as US regulatory requirements, US nuclear industry standards and functional specifications. The version of this document referenced from Ref. 12 is that developed for the standard **AP1000** plant design rather than a UK-specific version.

125. I found that the PMS BSC safety plan (Ref. 2) captures the need to update Ref. 12 to reflect a UK **AP1000** Requirements Traceability Matrix. This thereby ensures that, through implementation of this aspect of the safety plan early in the UK PMS development, Ref. 12 will reflect the UK design of the **AP1000** reactor. I have included the requirement to implement the safety plan in Assessment Finding CP-AF-AP1000-CI-018 in Section 4.2.2.7 below.

Final Quality Assessment and Justification Report – Addendum

126. The Final Quality Assessment and Justification (FQAJ) report (Ref. 30) provides an assessment of evaluations, analyses and complementary work for the qualification of the ABB AC160 as pre-developed software (PDS) according to IEC 60880, for earlier applications of the platform. The ONR Step 4 C&I assessment report (Ref. 7) describes the development of this report as a basis for justifying the AC160 software for use in support of Category A safety functions.

127. The FQAJ-A (Ref. 14) extends the FQAJ in order to cover the qualification of the extended scope and upgrades of the AC160 as applied in the **AP1000** PMS.

128. My review of the FQAJ-A (Ref. 14) included those Step 4 TOs that are addressed by the document. I used the PMS TO Traceability Matrix (Ref. 31) to determine those TOs that Westinghouse claimed are dealt with by the FQAJ-A. I sampled a number of TOs to determine whether they had been adequately addressed and used the PMS GDA Technical Observations Claims, Arguments and Evidence document (Ref. 32) to assist with understanding the CAE trail for the TOs in question.

129. Following my review of the FQAJ-A (Ref. 14), I raised a number of queries on RQ-AP1000-1722. Westinghouse responded to the RQ and subsequently provided a revision of the document. I found in the response to the RQ that a number of detailed points were not fully closed. These are captured under TOs CI-08-TO2-2.2.3.5.4-1 to -4 in Ref. 15. I am satisfied that the licensee may deal with these points during the design phase of the UK **AP1000** PMS development process and as such have captured the TOs under Assessment Finding CP-AF-AP1000-CI-018.

130. It should be noted that GDA Step 4 Assessment Findings AF-AP1000-CI-009 and AF-AP1000-CI-011 require the licensee to substantiate the software of the AC160 as follows:

> GDA Assessment Finding: **AF-AP1000-CI-009** – The licensee shall produce a comprehensive demonstration that the Added Quality Demonstration compensatory measures (i.e. the use of operating history, testing and static analysis) have adequately addressed the gaps identified during the qualification exercise for the original development of the AC 160 version 1.3/0. For further guidance see T15.TO1.03, T15.TO2.01 a, b and c, T15.TO2.03, T15.TO2.07, T15.TO2.08, T15.TO2.32, and T15.TO2.39 b and c in Annex 5.
>
> GDA Assessment Finding: **AF-AP1000-CI-011** - The licensee shall substantiate the claim of IEC 60880 compliance for the changes made to the AC 160 to create:
>
> - the AC 160 V1.3/0 nuclear baseline from the V1.2 software; and

- each subsequent AC 160 release (i.e. versions from V1.3/0 to V1.3/8).

The licensee shall document the change process used to create each of the software versions referenced above and demonstrate its adequacy.

The licensee shall ensure the demonstration of compliance with IEC 60880 addresses all relevant clauses such as change management, configuration control, software build, verification and test. The licensee shall demonstrate that the tests adequately addressed the modifications (e.g. the tests addressed the changes to the requirements and provided adequate code coverage). For further guidance, see T15.TO2.05, T15.TO2.06, T15.TO2.28, T15.TO2.34, T15.TO2.39 b, c and d, and T15.TO2.46 in Annex 5.

131. 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 these assessment findings.

132. While addressing the assessment findings above, the licensee should take account of the TOs raised in this assessment as captured in CP-AF-AP1000-CI-018.

Stonehouse Inspection of AC160 development documentation

133. In support of my assessment of the AC160 platform, I undertook an inspection of proprietary documentation at the ABB Stonehouse facility near Gloucester. This was the fourth such inspection at Stonehouse, the other three having taken place in earlier GDA steps.

134. The primary objective of this inspection was to review the evidence identified during the assessment of other documents submitted during the GDA issue close-out phase such as the FQAJ-A (Ref. 14) and the AC160 Suitability Analysis (Ref. 12).

135. I transmitted my sampling strategy and inspection schedule (Ref. 33) to Westinghouse in advance (who subsequently shared it with ABB) in order that the documentation may be prepared prior to my review. The sampling strategy considered the AC160 development process, the product itself and the configuration management applied.

136. The detailed findings from the inspection may be found in Ref 34. In summary I found that, in general, the objectives for the inspection were fulfilled. I found adequate evidence to support many of the Westinghouse claims and arguments for the AC160 platform, although there were gaps in a number of instances.

137. The most significant findings from the inspection included:

- The justification of the AC160 operating system (VRTX®) fell short of what is expected for a Class 1 system. The safety justification emphasised operational experience as a compensating measure for gaps in production excellence. The operational experience presented in support of this compensating measure had significant weaknesses and it was not clear what gaps the measure was filling.

- I identified gaps in the design and test lifecycle for the AC160 system software. The transition from architecture to code (the detailed design phase) was generally lacking in clarity, as was its related testing.

138. I raised a number of queries emerging from my inspection on RQ-AP1000-1768. The queries included a request for a justification of the VRTX® operating system that addressed the detailed findings of the inspection, including the consideration of further

compensating measures. I also requested that Westinghouse address the gaps identified in the design and test phases of the AC160 software lifecycle.

139. Following the Stonehouse inspection, Westinghouse initiated an information exchange with Mentor Graphics – the supplier of the VRTX® operating system. In its response to RQ-AP1000-1768, and in Section 4.3.1.15 of the PMS BSC safety plan (Ref. 2), Westinghouse explained that options for specific compensating measures for the gaps in production excellence will be driven by the availability of evidence and source code from the supplier. Westinghouse committed to a series of compensating measures depending upon the availability of the source code.

140. I reviewed the list of proposed compensating measures and, while it represents a step forward in providing a justification of VRTX® for use in a Class 1 system, a number of areas require further development. For example, in the event that the supplier does not make available VRTX® lifecycle documents, ONR would expect Westinghouse to regenerate the documentation to allow an independent derivation of software tests that can be confirmed to provide the code coverage necessary for a Class 1 system. I have captured these points of detail in the TOs referenced in Assessment Finding CP-AF-AP1000-CI-017 below.

141. I note that Step 4 Assessment Finding AF-AP1000-CI-009 requires the licensee to justify the use of the VRTX® operating system in the AC160 platform (T15.TO2.32). The licensee should implement the points raised in Assessment Finding CP-AF-AP1000-CI-017 below when addressing AF-AP1000-CI-009.

142. In its response to RQ-AP1000-1768, and in Section 4.3.1.10 of the PMS BSC safety plan (Ref. 2), Westinghouse also committed to perform a PMS Requirements Traceability Matrix process in order to reconstitute the V-model for each AC160 software partition. Gaps identified in the V-model documentation (including those from my inspection) will be closed by re-engineering the missing documents and, as necessary, additional test cases and reports. A number of exceptions to this approach, including the VRTX® operating system, are identified. Alternative justification approaches are captured for such exceptions. I am satisfied that this commitment addresses the concern raised at the inspection. The assessment finding below requires the licensee to fulfil this commitment and to address the points of detail associated with this issue as identified in TO CI-08-TO2-2.2.4.8-6 in Ref. 15.

143. I have raised the assessment finding below to capture those matters arising from the Stonehouse inspection that need to be addressed during the implementation of the PMS using the ABB AC160 platform.

> GDA Assessment Finding: **CP-AF-AP1000-CI-017** – The licensee shall address the findings from the ONR Stonehouse inspection of the ABB AC160 software development process and product including but not limited to:
>
> - Justify the VRTX® operating system for use in a Class 1 system; and
> - Address the gaps identified in the AC160 software lifecycle.
>
> See TOs CI-08-TO2-2.2.4.8-1 to -10 in Ref. 15 for further guidance on addressing the findings from the Stonehouse inspection.

4.2.2.7 Summary of Assessment of GDA Issue Action GI-AP1000-CI-08.A2 – Provision of a BSC for the PMS

144. GDA issue action GI-AP1000-CI-08.A2 requires the provision of a BSC for the UK **AP1000** PMS that takes into account ONR expectations for such a document. Those expectations are described in the action itself and in Ref. 16.

145. I have assessed the PMS BSC (Ref. 2), its key supporting documents and sampled their references. I have confirmed that this action has been adequately addressed and may be closed.

146. I found that the structure and content of the PMS BSC (Ref. 2), together with the key supporting references, was adequate to meet my expectations in terms of coverage of BSC topics and elements as outlined in the GDA issue and the supporting guidance. I identified a number of issues with the BSC and its supporting documents that do not prevent closure of the GDA issue action, but require resolution during the development of the PMS post GDA. I have captured these issues in Assessment Finding CP-AF-AP1000-CI-018 below.

147. I note that the PMS safety case documentation, including the BSC and its supporting references, will be updated as the UK **AP1000** PMS development lifecycle (from concept / planning to operations and maintenance) is implemented post GDA. The activities and timescales for this process are described in the PMS BSC safety plan. I judge that it is appropriate to implement those activities identified in the safety plan post GDA.

148. I have captured the requirement for the licensee to complete the safety case documentation for the UK **AP1000** PMS, to address the findings of my assessment and to implement those activities identified in the safety plan in the assessment finding below:

> GDA Assessment Finding: **CP-AF-AP1000-CI-018** – The licensee shall fully develop the safety case outlined in the PMS BSC and its supporting documents and implement the BSC safety plan (Ref. 2). This shall include but not be limited to:
>
> - Justify the final PMS design including use of the AC160 platform in the safety case;
> - Implement the compensating measures including those in the SAP and standards compliance matrices; and
> - Justify the Programmable Complex Electronic Components in the AC160 platform.
>
> For further guidance on the completion of the PMS safety case, see Step 4 Assessment Finding AF-AP1000-CI-010 and Technical Observations CI-08-TO2-2.2.2.9.4-1 to -5, CI-08-TO2-2.2.2.6.4-1, CI-08-TO2-2.2.2.7.4-1 and -2, GI-08-TO2-2.2.2.2.4-1, CI-08-TO2-2.2.2.4.6-1, CI-08-TO2-2.2.2.4.6-3, CI-08-TO2-2.2.3.3.4-1, CI-08-TO2-2.2.3.4.4-1 and -2, CI-08-TO2-2.2.3.5.4-1 to -4, CI-08-TO2-2.2.2.1.4-1 and CI-08-TO2-2.2.2.8.4-1 in Ref.15.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

149. My assessment has included consideration of whether the Westinghouse submissions meet the expectations of relevant standards, guidance and good practice. This

assessment is described in the sections above (e.g. see assessment of SAPs CAE submission (Ref. 8) and standards compliance submissions (Refs 9, 10, 11 and 13)). I am content that Westinghouse has made satisfactory use of relevant standards, guidance and good practice.

4.4 Assessment Findings

150. During my assessment eight items were identified for a future licensee to take forward in its site-specific safety submissions. Details of these are contained above and in Annex 1.

151. 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.

152. 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; and
- 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).

5 CONCLUSIONS

153. This report presents the findings of my assessment of GDA Issue GI-AP1000-CI-08 Revision 0 PMS Adequacy of Safety Case relating to the **AP1000** GDA closure phase.

154. 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).

155. 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-08 Revision 0 PMS Adequacy of Safety Case.

156. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-08 may be closed.

REFERENCES

1. ONR-GDA-AP-14-001 Rev 0, AP1000 GDA C&I Assessment Plan, April 2015. TRIM 2015/149263

2. UKP-PMS-GLR-001 Rev 2, United Kingdom AP1000® Protection and Safety Monitoring System Safety Case Basis, December 2016. TRIM 2016/502555

3. Resolution Plan for GI-AP1000-C&I-08 PMS BSC Rev 3, February 2016. TRIM 2016/92098

4. NS-PER-GD-014 Rev 5, Purpose and Scope of Permissioning, August 2015. TRIM 2015/304735

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

6. Office for Nuclear Regulation (ONR) Permissioning inspection, Technical assessment guides. www.onr.org.uk/operational/tech_asst_guides/index.htm

7. ONR-GDA-AR-11-006 Rev 0, Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor, November 2011. TRIM 2010/581525

8. UKP-PMS-GL-010 Rev 2, United Kingdom AP1000 PMS Safety Assessment Principles Evaluation, December 2016. TRIM 2016/492569

9. UKP-PMS-GL-012 Rev 1, United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Protection and Safety Monitoring System, December 2016. TRIM 2016/482514

10. UKP-PMS-GL-002 Rev 2, United Kingdom AP1000 IEC 60880 Compliance Matrix for the Protection and Safety Monitoring System, July 2016. TRIM 2016/295083

11. UKP-PMS-GLR-007 Rev 1, United Kingdom AP1000 IEC 60987 Compliance Matrix for the Protection and Safety Monitoring System, July 2016. TRIM 2016/276470

12. UKP-PMS-GL-005 Rev 1, United Kingdom AP1000 Protection and Safety Monitoring System AC160 Suitability Analysis, December 2016. TRIM 2016/474772

13. WEG-AR-00579-GEN Rev 00, IEC 60987 Compliance Matrix for the AC160 Product HW as integral part of the Protection and Safety Monitoring System, July 2016. TRIM 2016/426800

14. GBRA095803 Rev. D, O1-MOD – Qualification Final Quality Assessment and Justification Report – Addendum, December 2016. TRIM 2016/485069

15. S.P1641.40.TSC267.6 Issue 1.0, ONR/T2723: Support for AP1000 C&I GDA Issues resolution, Review of Submissions for the closure of GDA Issue 08 PMS – Adequacy of Safety Case, February 2017. TRIM 2017/80938

16. C&I GDA Issues Closure Guidance Document Rev 0. TRIM 2015/84414

17. ONR-WEC-0006N, C&I GDA Issues Closure Guidance Document Covering Letter. TRIM 2015/84411

18. ONR-NR-AR-16-035 Rev 0, ONR Assessment Report - GDA close-out for the AP1000 Reactor, GDA issue GI-AP1000-CI-09 Component Interface Module – Adequacy of Safety Case, March 2017. TRIM 2016/274947

19. ONR-NR-AR-16-031 Rev 0, ONR Assessment Report – GDA close-out for the AP1000 Reactor, GDA issue GI-AP1000-CI-04 – PMS Spurious Operation, March 2017. TRIM 2016/274942

20. APP-PMS-AR-001 Rev 2, AP1000 Protection and Safety Monitoring System Reliability Analysis, October 2015. TRIM 2016/209677

21. ONR-NR-AR-16-017 Rev 0, GDA close-out for the AP1000 Reactor, Probabilistic Safety Analysis for the Westinghouse AP1000© Reactor. GDA issue GI-AP1000-PSA-01. Success Criteria (Internal Events At-Power), March 2017. TRIM 2016/275018

22. ONR RQ Tracking Sheet - TRIM 2016/383615

23. APP-GW-G1-011 Rev 7, AP1000® Plant Metrication Strategy and ALARP Assessment for the United Kingdom, November 2016. TRIM 2016/450594

24. ONR-GDA-CR-15-156, ONR Contact Record, AP1000 C&I GDA Issues Resolution – Progress Meeting, August 2015. TRIM 2015/293778

25. ONR-NR-CR-16-825, ONR Contact Record, AP1000 C&I GDA Issues Resolution – Progress Meeting, December 2015. TRIM 2016/499847

26. 204345-0000-DG00-RPT-0001 Issue 9, AP1000 Statistical Testing Plan Approach, December 2016. TRIM 2016/495767

27. 204345-0000-DG00-RPT-0004 Issue 8, UK AP1000 PMS Statistical Testing – Test Plan, September 2016. TRIM 2016/495780

28. ONR Note for the Record, Close-out of C&I GDA Issues – GDA Issue GI-AP1000-CI-08, Review of WEC Submissions – AP1000 Statistical Testing Plan Approach – 204345-0000-DG00-RPT-0001 and UK AP1000 PMS Statistical Testing – Testing Plan, 204345-0000-DG00-RPT-0004, Rev. 0, December 2016. TRIM 2016/496984

29. APP-PMS-J0R-001 Rev. 3, AP1000 Protection and Safety Monitoring System Requirements Traceability Matrix, October 2015. TRIM 2016/361682

30. MOD 97-7771 Rev. 6, Oskarshamn 1 – Project Mod Qualification of Category A I&C Final Quality Assessment and Justification Report, May 2002. TRIM 2011/401604

31. WEC-REG-0398N, Enclosure 1, PMS TO Traceability Matrix, October 2015. TRIM 2015/394389

32. UKP-PMS-GL-016 Rev 1, United Kingdom AP1000 PMS GDA Technical Observations Claims, Arguments and Evidence, December 2016. TRIM 2016/502558

33. Technical Guidance Note 9, ONR/T2723: Support for AP1000 C&I GDA Issues Resolution, AC160 (SH4) Sampling Strategy and Inspection Schedule, October 2016. TRIM 2016/421459

34. S.P1641.40.TSC267.6.1 Issue 1.0, ONR/T2723: Support for AP1000 C&I GDA Issues resolution, ABB, AC160 (SH4) Inspection Report, November 2016. TRIM 2016/454024

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-011	The licensee shall justify the reliability of the detailed PMS design in the safety case including but not limited to: • provide a probability of failure on demand figure for each individual safety function which includes all sources of random, common mode and systematic failures; • provide a justification for the beta factors and test intervals used in the reliability analysis that is based on the UK **AP1000** detailed design and implementation; and • update the overall UK **AP1000** plant PSA, as necessary, to reflect the as-designed reliability calculations.	4.2.2.1
CP-AF-AP1000-CI-012	The licensee shall justify the final PMS architecture and detailed design taking into account the re-categorisation of safety functions and the modifications recommended in the BSC safety plan (Ref. 2). For guidance on this assessment finding see also Step 4 Assessment Finding AF-AP1000-CI-024.	4.2.2.2
CP-AF-AP1000-CI-013	The licensee shall justify the final as-built PMS software associated with the derivation and conversion of set-points and engineering units.	4.2.2.3
CP-AF-AP1000-CI-014	The licensee shall implement a statistical test programme for the PMS that includes but is not limited to: • regression testing following software modifications;	4.2.2.4

	• definition and justification of linearisation curves and noise factors; and • definition and justification of test reset characteristics including reset periods. For further guidance on this assessment finding, see Ref. 28.	
CP-AF-AP1000-CI-015	The licensee shall address all “should” and “may” statements in all standards conformance assessments for the PMS. For further guidance on this assessment finding see also Step 4 Assessment Finding AF-AP1000-CI-05 and CI-08-TO2-2.2.2.4.6-2 in Ref. 15.	4.2.2.6
CP-AF-AP1000-CI-016	The licensee shall justify that the selected operating system for use with the Flat Panel Display System (FPDS) meets Class 1 requirements. For further guidance on the completion of the FPDS operating system justification see Technical Observation CI-08-TO2-2.2.2.4.6-4 in Ref. 15.	4.2.2.6
CP-AF-AP1000-CI-017	The licensee shall address the findings from the ONR Stonehouse inspection of the ABB AC160 software development process and product including but not limited to: • Justify the VRTX® operating system for use in a Class 1 system; and • Address the gaps identified in the AC160 software lifecycle. See TOs CI-08-TO2-2.2.4.8-1 to -10 in Ref. 15 for further guidance on addressing the findings from the Stonehouse inspection.	4.2.2.6
CP-AF-AP1000-CI-018	The licensee shall fully develop the safety case outlined in the PMS	4.2.2.7

	BSC and its supporting documents and implement the BSC safety plan (Ref. 2). This shall include but not be limited to: • Justify the final PMS design including use of the AC160 platform in the safety case; • Implement the Compensating Measures including those in the SAP and standards compliance matrices; and • Justify the Programmable Complex Electronic Components in the AC160 platform. For further guidance on the completion of the PMS safety case, see Step 4 assessment finding AF-AP1000-CI-010 and Technical Observations CI-08-TO2-2.2.2.9.4-1 to -5, CI-08-TO2-2.2.2.6.4-1, CI-08-TO2-2.2.2.7.4-1 and -2, GI-08-TO2-2.2.2.2.4-1, CI-08-TO2-2.2.2.4.6-1, CI-08-TO2-2.2.2.4.6-3, CI-08-TO2-2.2.3.3.4-1, CI-08-TO2-2.2.3.4.4-1 and -2, CI-08-TO2-2.2.3.5.4-1 to -4, CI-08-TO2-2.2.2.1.4-1 and CI-08-TO2-2.2.2.8.4-1 in Ref. 15.	