New Reactors Programme

GDA close-out for the AP1000®pressurised water reactor

GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case

Assessment Report: ONR-NR-AR-16-033
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 the award of a Design Acceptance Confirmation (DAC) and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report is 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 issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, Distributed Control and Information System (DCIS) Adequacy of Safety Case.

This GDA issue arose in Step 4 due to the need to:

- improve the quality of the safety case for the DCIS, which comprises the Plant Control System (PLS) and Data Display and Processing System (DDS);
- improve the quality of the Ovation platform safety justification;
- provide access to the evidence supporting the safety justifications.

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

- provide DCIS Basis of Safety Case (BSC) documents for the Class 2 PLS and Class 3 DDS that meet ONR expectations;
- provide compliance documents for the tier 1 IEC standards and ONR Safety Assessment Principles (SAPs);
- provide a documentation package that justifies qualification of the Ovation platform for Class 2 and 3 applications;
- make available further documents that support the BSCs as requested by ONR;
- provide in the BSCs a programme plan for the UK PLS/DDS that makes visible the development of the BSC in line with the design.

My assessment conclusion is:

- the safety case for the PLS and DDS has been significantly improved through the provision of the BSCs and references;
- the justification for the Ovation platform has been significantly improved through the provision of a documentation package that includes the results of an audit of the supplier (commercial grade survey);
- Westinghouse has made appropriate use of modern standards and safety principles in the BSCs and justification of the Ovation platform.

My judgement is based upon the following factors:

- review of the PLS and DDS BSCs and key supporting submissions as identified in the resolution plan and sampling of selected references to these documents;
- adoption by Westinghouse of International Electrotechnical Commission (IEC) standards for the design of the PLS and DDS applications and satisfaction of key ONR SAPs;
- adoption by Westinghouse of IEC standards as the basis for the commercial grade survey of the Ovation platform;

- the explicit inclusion of compensating measures (CMs) to provide conformance to IEC standards and SAPs in Westinghouse's PLS and DDS BSC safety plans for the development of the PLS and DDS post-GDA.

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

- fully develop the safety case outlined in the PLS and DDS BSCs (for example, by implementing the safety plans contained in the BSCs) as the detailed design and implementation of the systems is completed post GDA;
- complete the substantiation of the adequacy of the Ovation platform following selection of the Class 2 and 3 components to be used for the UK **AP1000** reactor design, including inspection of the suppliers (Westinghouse and Emerson the Ovation platform supplier);
- implement the CMs identified in the SAPs and standards compliance submissions (for the systems and platform) by, for example, including design and implementation details such as verification, validation and commissioning test records;
- document and justify the reliability of the final detailed PLS and DDS designs in the safety cases.

These outstanding matters have been identified as assessment findings. These matters do not undermine the generic safety submission and require licensee input/decision.

In summary I am satisfied that GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case can be closed.

LIST OF ABBREVIATIONS

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
CM	Compensating Measure
COTS	Commercial Off-The-Shelf
DCIS	Distributed Control and Information System
DDS	Data Display and Processing System
FMEA	Failure Modes and Effects Analysis
GDA	Generic Design Assessment
HDL	Hardware Description Language
HPD	HDL Programmed Devices
HVAC	Heating, Ventilation and Air Conditioning
ICBM	Independent Confidence Building Measure
IEC	International Electrotechnical Commission
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PCSR	Pre-Construction Safety Report
pdfy	Probability of Dangerous Failures per Year
PE	Production Excellence
PLS	Plant Control System
PSA	Probabilistic Safety Assessment
RBD	Reliability Block Diagram
RGP	relevant good practice
RNS	normal residual heat removal system
RP	Requesting Party
RQ	Regulatory Query
RTOS	Real-Time Operating System
SAPs	Safety Assessment Principles
SSC	System, Structure (and) Component
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor

TABLE OF CONTENTS

1 INTRODUCTION 7
1.1 Background 7
1.2 Scope 7
1.3 Method 8
2 ASSESSMENT STRATEGY 9
2.1 Pre-Construction Safety Report (PCSR) 9
2.2 Standards and Criteria 9
2.3 Use of Technical Support Contractors (TSCs) 11
2.4 Integration with Other Assessment Topics 12
2.5 Out of Scope Items 12
3 REQUESTING PARTY'S SAFETY CASE 14
4 ONR ASSESSMENT OF GDA ISSUES GI-AP1000-CI-06 REVISION 0, OVATION PLATFORM ADEQUACY OF SAFETY CASE AND GI-AP1000-CI-07 REVISION 0, DCIS ADEQUACY OF SAFETY CASE 15
4.1 Scope of Assessment Undertaken 15
4.2 Assessment 15
4.3 Comparison with Standards, Guidance and Relevant Good Practice 33
4.4 Assessment Findings 33
5 CONCLUSIONS 35
6 REFERENCES 36

Tables

Table 1 – Key Safety Assessment Principles
Table 2 – Technical Assessment Guides
Table 3 – National and International Standards and Guidance
Table 4 – Work Packages Undertaken by the TSC
Table 5 – Availability of PLS and DDS Documentation for GDA Assessment

Annex

Annex 1: Assessment Findings to be addressed during the Forward Programme – Control and Instrumentation

1 INTRODUCTION

1.1 Background

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

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse AP1000®pressurised water reactor design in the area of Control and Instrumentation (C&I). Specifically this report addresses GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, Distributed Control and Information System (DCIS) Adequacy of Safety Case.

3. Westinghouse explained that DCIS is its generic control system terminology and the Plant Control System (PLS) and Data Display and Processing System (DDS) are the implementation of the DCIS for the UK **AP1000** plant. Therefore, in response to the GDA issues, Westinghouse submitted separate Basis of Safety Cases (BSCs) for the PLS and DDS, which address for each system both Westinghouse's application development and Ovation platform substantiation. The GDA issues requested the provision of BSCs for the Ovation platform (GDA Issue Action GI-AP1000-C&I-06.A2) and PLS/DDS application (GDA Issue Action GI-AP1000-C&I-07.A2). I accept that the approach adopted by Westinghouse provides a logical means by which to structure the safety justifications.

4. The related GDA Step 4 report is published on our website (**www.onr.org.uk/new-reactors/ap1000/reports.htm**), and 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

5. The scope of this assessment is detailed in the assessment plan AP1000 GDA C&I Assessment Plan ONR-GDA-AP-14-001 Rev 0, (Ref. 60).

6. The scope of my assessment focussed on the:

   - PLS and DDS BSCs, which provide justification of the suitability of the PLS application at Class 2 (for example, automatic control) and the DDS application at Class 3 (manual control and display) (action GI-AP1000-C&I-07.A2);
   - detailed evidence used to support the BSCs for the PLS and DDS applications (action GI-P1000-C&I-07.A1);
   - PLS and DDS BSCs, which include justification of the suitability of the Ovation platform for Class 2 and 3 systems (action GI-AP1000-C&I-06.A2);
   - detailed evidence used to support the Ovation platform justification (action GI-AP1000-C&I-06.A1) such as the commercial grade survey report and its references.

7. My assessment addressed the need for Westinghouse to improve the quality of the PLS and DDS safety cases, and the justification of the Ovation platform through the submission of BSCs and supporting references, which were the key areas of concern identified during GDA Step 4. Westinghouse's GDA submissions should be consistent

in terms of scope and content with those of a Pre-Construction Safety Report (PCSR) but the Step 4 submissions (see Ref. 17) fell short of this expectation.

8. The scope of assessment is appropriate for GDA because it ensured an adequate safety justification was set out prior to the detailed design and implementation phases of the PLS and DDS lifecycle, thereby reducing the risk that significant safety issues will arise post-GDA. The scope of assessment is proportionate since it provides a review of the detail expected to be provided in a PCSR and its supporting references such as the PLS and DDS BSCs (see ONR Guidance to Requesting Parties (Ref. 59)). In addition, the assessment focused on key areas such as SAPs and nuclear sector standards conformance demonstrations that Westinghouse needed to address in order to close out the GDA issues.

1.3 Method

9. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 1).

1.3.1 Sampling Strategy

10. 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 PLS and DDS BSCs and sample key references and supporting submissions identified in the Westinghouse resolution plan and BSCs. I adopted a risk-based approach whereby I allocated more assessment resource to the review of the Class 2 PLS than the Class 3 DDS (as reflected in the reviews recorded below). It is important that the BSCs meet the expectations for a BSC outlined in the GDA issue. I included a review of the BSCs to confirm that they met the expectations outlined in the GDA issues. I also considered it important that the BSCs and supporting submissions demonstrate conformance to ONR SAPs and key International Electrotechnical Commission (IEC) nuclear sector standards. My review also included consideration of whether Westinghouse followed relevant good practice (RGP) and completion of Step 4 Technical Observations (TOs) identified under the GDA issues. I included specific sampling of submissions in these areas in my review.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

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 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** reactor's 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 issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case.

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) (Ref. 15), internal TAGs (Ref. 16), 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 the assessment are included 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 Ref. 17 (Table 4).

Table 1 – Key Safety Assessment Principles

ESS.27	Computer-based safety systems
ESR	Safety-related systems (Class 2 and 3)
ESR.1	Provision in control rooms and other locations
ESR.2	Performance requirements
ESR.3	Adequate and reliable controls
ESR.4	Minimum operational equipment
ESR.5	Standards for equipment in safety-related systems
ESR.6	Power supplies
ESR.9	Response of control systems to normal plant disturbances
ESR.10	Demands on safety systems in the event of control system faults
ECS.1, 2 & 3	Categorisation and classification
EQU.1	Qualification procedures
EDR.1	Design for reliability

EDR.2	Failure to safety
EDR.3	Common cause failure (CCF) – use of common components to deliver required integrity
ERL.1	Form of claims
ERL.2	Measures to achieve reliability
EMT.1	Identification of requirements
EMT.2	Frequency
EMT.3	Type-testing
EMT.5	Procedures/commissioning
EMT.6	Reliability claims
EMT.7	Functional testing
EAD.1	Safe working life
EAD.5	Obsolescence
ECM.1	Commission testing
EHF.7	User interfaces

2.2.2 Technical Assessment Guides

16. The TAGs that has been used as part of this assessment are set out in Table 2.

Table 2 – Technical Assessment Guides

NS-TAST-GD-031 (Rev 4)	Safety Related Instrumentation
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 as part of this 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.
IEC 61513:2011	Nuclear power plants. Instrumentation and control for systems important to safety. General requirements for systems.
IEC 61508:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems.
IEC 62340:2010	Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure (CCF).

IEC 60987:2007 + A1:2013	Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems.
IEC 62138:2004	Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.

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, enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision making, and so on.

19. Table 4 sets out the broad areas where technical support was used. This support was required to provide additional capacity and enable 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 Technical Support Contractor

TSC	Work Package
Altran UK Ltd	Review of PLS BSC (Ref. 3) and key references (SAP CAE (Ref. 4) and IEC 61513 CAE (Ref. 5)) plus sampling of selected references identified during the reviews of Refs. 3, 4 and 5.
"	Review of IEC 62138 Compliance Matrix for the PLS (Ref. 6).
"	Review of IEC 60987 Compliance Matrix for the PLS (Ref. 7).
"	Review of DDS Basis of Safety Case (Ref. 8) and key references (SAP CAEs (Ref. 9) and IEC 61513 CAE (Ref. 10)) plus sampling of selected BSC references.
"	Review of IEC 62138 Compliance Matrix for the DDS (Ref 11).
"	Review of Commercial Dedication Plan (Ref. 12), Report (Ref. 13) and Instruction (Ref. 14).

20. 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** reactor was made exclusively by an ONR inspector. 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 (TRIM) can be identified through Ref. 21.

21. The TSC has provided a report (Ref. 18) that addresses the scope of work listed above. The TSC also reviewed responses to RQs and meeting actions placed on Westinghouse. Ref. 18 includes a summary statement of the results of the TSC's work and findings (Technical Observations (TOs)). I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under assessment findings (see Annex 1).

The TSC TOs provide further guidance on the GDA assessment findings and their means of resolution. Within this report references to the TSC TOs contained in Ref. 18 are provided using the unique TO identifiers (for example, CI-xx.TO1/2-mmmm.nn, where mmmm is the Ref. 18 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 this assessment, I consulted with an ONR PSA inspector in relation to modelling of PLS/DDS reliability in the Probabilistic Safety Assessment (PSA). I consulted an ONR Fault Studies inspector in relation to the categorisation of PLS/DDS functions and the context of assessment findings AF-AP1000-FS-01, 02 and 03 (see below).

2.5 Out of Scope Items

23. The items (systems and safety case documentation) that are outside the scope of GDA are identified in the Step 4 C&I assessment report Ref. 17. The availability of evidence is identified in Ref. 17 as:

- 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 (for example, documents and reports) from that phase are available to ONR for assessment; and
- C – neither the documentation that specifies the process nor the output products for that phase are available to ONR for assessment.

24. For the Ovation platform the ‘Platform Description’ is ‘A’ and ‘Platform Qualification’ is ‘B’. In relation to the implementation of the PLS and DDS using the Ovation platform, the availability of documentation for GDA assessment declared by Westinghouse (see Ref. 17) is as shown below in Table 5.

Table 5 – Availability of PLS and DDS Documentation for GDA Assessment

Lifecycle Phase	Availability PLS	Availability DDS
Design Requirements	A	A
System Definition	B	B
Design	B	B
Implementation	B	B
Test	B	B
Installation	C	C

25. The level of detail is considered acceptable as it aligns with that expected for a PCSR at the GDA stage and recognises that the PLS and DDS using the Ovation platform will need to be developed to meet the specific needs of the UK **AP1000** reactor project. Westinghouse made exemplar documents from other Westinghouse projects available for review.

3 REQUESTING PARTY'S SAFETY CASE

26. Westinghouse's safety case for the PLS and DDS is based on the presentation of adequate BSC documents that, along with supporting references, demonstrate that the GDA issues have been satisfactorily addressed. As noted above, the BSCs for the PLS and DDS address both the application and Ovation platform. The Westinghouse safety case for GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case is documented in:

- United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case – UKP-PLS-GLR-001, Rev. 0 (Ref. 3), which is the main submission addressing the GDA issues in respect of the PLS;
- key references to the PLS BSC, including those identified in the Westinghouse resolution plan,
    - United Kingdom AP1000 Plant Control System (PLS) Safety Assessment Principle Compliance – UKP-PLS-GLR-002, Rev. 0 (Ref 4),
    - United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Plant Control System (PLS) – UKP-PLS-GLR-003, Rev. 0 (Ref. 5),
    - United Kingdom AP1000 IEC 62138 Compliance Matrix for the Plant Control System – UKP-PLS-GL-002, Rev. 0 (Ref. 6),
    - United Kingdom AP1000 IEC 60987 Compliance Matrix for the Plant Control System – UKP-PLS-GL-001, Rev. 0 (Ref. 7);
- United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case UKP-DDS-GLR-001, Rev. 0 (Ref. 8), which is the main submission addressing the GDA issues in respect of the DDS;
- key references to the DDS BSC including those identified in the Westinghouse resolution plan,
    - United Kingdom AP1000 Data Display and Processing System (DDS) Safety Assessment Principle Compliance – UKP-DDS-GLR-002, Rev. 0 (Ref. 9),
    - United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Data Display and Processing System (DDS) – UKP-DDS-GLR-003, Rev. 0 (Ref. 10),
    - United Kingdom AP1000 IEC 62138 Compliance Matrix for the Data Display System – UKP-DDS-GL-001, Rev. 0 (Ref. 11);
- Ovation commercial grade survey documents that support Refs. 3 and 8 in relation to the justification of the Ovation platform,
    - Distributed Control and Information Systems - Systems Important to Safety - Commercial Dedication Plan – WNA-PV-00075-GEN, Rev. 0 (Ref. 12),
    - Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Report for the Ovation 3.5.1 Platform – WNA-VR-00464-GEN, Rev. 0 (Ref. 13),
    - Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Instruction – Ovation 3.5.1 Controller Complementary Testing -WNA-CD-00048-GEN, Rev. 0 (Ref. 14).

4 ONR ASSESSMENT OF GDA ISSUES GI-AP1000-CI-06 REVISION 0, OVATION PLATFORM ADEQUACY OF SAFETY CASE AND GI-AP1000-CI-07 REVISION 0, DCIS ADEQUACY OF SAFETY CASE

27. 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

28. The scope of the assessment covered the Westinghouse submissions identified in the GDA issue resolution plan (Ref. 2). This included the PLS and DDS BSCs (Refs. 3 and 8), SAP compliance (Refs. 4 and 9), IEC 61513 CAEs (Refs. 5 and 10), standards compliance matrices (Refs. 6, 7 and 11) and Ovation commercial grade survey documents (Refs. 12, 13 and 14). Following my review of Westinghouse's initial submissions, Westinghouse provided revised submissions as necessary to capture the clarifications and commitments made in the various RQ responses. I describe the progression of the submitted documents in the sections below. I also sampled supporting submissions referenced from the main submissions above, and I discuss my assessment of these supporting submissions below.

29. The submissions made by Westinghouse in this area may address GDA Step 4 assessment findings (see Ref. 17). 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.

4.2 Assessment

30. I discuss my assessment of Westinghouse's submissions provided in response to GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case below. I reviewed the initial submissions and raised clarification requests by RQ. As appropriate, Westinghouse revised the submitted documents to address the RQ points. The description of the scope of work performed by the TSC and the TOs arising from their work are contained in a TSC report (Ref. 18).

31. The PLS and DDS provide the main control and display system for the **AP1000** reactor. The PLS includes the main closed loop controls necessary for plant operation, including reactor power control, pressuriser pressure and level control, and steam generator level control. The DDS provides facilities for operator controls, displays and alarms for normal plant operations. The PLS and DDS are treated as non-safety systems in the classification scheme used by Westinghouse for the generic US design of the standard **AP1000** plant. Following the functional categorisation and system classification approach recognised in the UK, as outlined in IEC 61226 and IEC 61513, the PLS is classified as Class 2 and the DDS as Class 3 for the UK **AP1000** plant. This classification assists with the selection of appropriate IEC nuclear sector standards and relevant sections/clauses therein.

32. Westinghouse originally developed control platforms for plant automation applications including those of nuclear facilities. Emerson has taken over the Ovation platform development over the last decade, working to commercial rather than nuclear-specific standards. The GDA Step 4 assessment revealed that there was very little detailed documentary evidence available for review that would support a Class 2 (PLS) and Class 3 (DDS) safety demonstration.

33. GDA issue GI-AP1000-CI-07, DCIS Adequacy of Safety Case states "AP1000 automatic and manual controls, and displays are provided by the DCIS (PLS/DDS). Elements of the DCIS have to be justified as Class 2 (PLS) and Class 3 (DDS)

respectively as part of the plant safety case. This requires a new justification as the systems are given a non-safety classification in the US". To address this GDA issue, Westinghouse needed to respond to actions GI-AP1000-CI-07.A1 and A2. GDA issue: GI-AP1000-CI-06 Ovation Platform Adequacy of Safety Case states "Westinghouse to provide an adequate safety case for the Ovation platform that supports the Class 2 closed loop controls and the Class 3 manual controls and displays of AP1000". Westinghouse needed to respond to actions GI-AP1000-CI-06.A1 and A2. In response to the GDA issues, Westinghouse has submitted BSCs for the PLS and DDS, which address each system in terms of both application and platform. I discuss my assessment of Westinghouse's response to these actions below.

4.2.1 Westinghouse to facilitate ONR access in the UK to the detailed BSC evidence (GI-AP1000-CI-06.A1 and GI-AP1000-CI-07.A1)

34. GI-AP1000-CI-06.A1 and GI-AP1000-CI-07.A1 required Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the BSCs for the PLS and DDS applications**,** and the Ovation platform. Westinghouse has made all PLS and DDS documents available to ONR in the UK. The formal documents identified in the resolution plan were submitted as they became available and in accordance with Westinghouse's rescheduled submission programme. Westinghouse submitted further supporting documents to ONR on RQ request. Westinghouse provided access to Emerson documents in line with a documented request process (Ref. 22). I reviewed commercially-sensitive supplier evidence at an Emerson facility in the UK (see discussion of the Ovation platform inspection in section 4.2.2.3). Because of the access to documents provided in the UK, GDA actions GI-AP1000-CI-07.A1 and GI-AP1000-CI-06.A1 are closed.

4.2.2 Provision of PLS, DDS and Ovation platform BSCs (GI-AP1000-CI-06.A2 and GI-AP1000-CI-07.A2)

35. In this section, I present an overview of GDA issue actions GI-AP1000-CI-06.A2 and GI-AP1000-CI-07.A2, which required Westinghouse to provide DCIS and Ovation platform BSCs. Westinghouse chose to structure its safety submissions such that a BSC was submitted that provided justification of the PLS application and Ovation platform to Class 2. Westinghouse provided a separate BSC for the justification of the DDS application and Ovation platform to Class 3. This section and the sections below describe the review of the submissions provided in response to these GDA issue actions.

36. I undertook the review of Refs. 3 and Ref. 8 to confirm whether the submissions adequately address the topics and elements of a BSC as outlined in the GDA issues and ONR GDA Issues Closure Guidance Document (Ref. 19). I also checked whether Westinghouse had adequately addressed the IEC 61513 safety lifecycle (section 6) for the PLS and DDS. I had supplied Ref. 19 to Westinghouse as additional guidance and in the letter supplying this document (Ref. 20), I explained to Westinghouse that it is the Requesting Party's (RP) responsibility to consider and provide a comprehensive safety submission addressing each of the GDA issues.

37. The PLS and DDS BSCs (Refs. 3 and 8) provide system descriptions in section 3. Section 4 contains a safety plan that outlines future safety case activities, including a description of how and when Westinghouse will implement the compensating measures identified in their SAPs and standards compliance assessments (for example, by including design and implementation detail). The safety plan also includes discussion of how Westinghouse addressed Step 4 assessment findings and TOs. Section 5 provides the demonstration of conformance to a safety lifecycle (for example, through conformance to IEC 61513 and IEC 62138). Section 5.1 defines the applicable SAPs and the Compensating Measures (CMs) required for the systems to conform to the SAPs. CMs arising from the IEC 61513 and IEC 62138 conformance

demonstrations are presented in sections 5.2 and 5.3 respectively. For the PLS, CMs arising from the IEC 60987 conformance demonstration are presented in section 5.4. The PLS BSC section 5.5 presents and DDS BSC section 5 references (for example, through gaps identified in Table 5-4) the Ovation platform commercial dedication CMs. Section 6 of the BSCs address safety lifecycle supporting activities (for example, the Westinghouse quality management system and Independent Confidence Building Measures (ICBMs)). Section 7 of the BSCs presents the ALARP argument (for example, discussing how the systems incorporate relevant good practice and the design options considered).

38. Note that the detail of the CAE for conformance to the SAPs and standards conformance demonstrations is not contained in the BSCs but is provided in separate documents (Refs. 4, 5, 6, 7 and 13 for the PLS and Refs. 9, 10 and 11 for the DDS, see below).

39. I found (in Ref. 18) that the structure of the PLS and DDS BSCs (Refs. 3 and 8), together with the key supporting references, broadly met my expectations in terms of BSC topics and elements as outlined in the GDA issues.

40. The safety case documentation (for example, BSC and conformance assessments) will be updated as the detailed design of the PLS and DDS is finalised and implemented post-GDA (for example, to document closure of the gaps identified in the safety plans). The implementation detail for the PLS and DDS design presented during GDA is not complete; however, it is sufficient to demonstrate that no significant safety issues remain. I am content that it is appropriate to address the conformance demonstration gaps post-GDA, as they require the provision of evidence that will become available at that time.

4.2.2.1 PLS Application Assessment

41. This section presents my assessment of Westinghouse's response to GDA issue action GI-AP1000-C&I-07.A2 on the PLS application. I present an overview of Ref. 3's structure and content above. The overall PLS safety claim (Ref. 3, claim C.1) is that the PLS has an adequate safety demonstration to maintain stable conditions in normal plant operation, and prevent deviations from normal operation leading to the initiation of the protection systems (PMS and DAS). Following my review of the PLS BSC (Ref. 3), I raised a number of application related queries in RQ-AP1000-1669 and RQ-AP1000-1701. For example, for Westinghouse to clarify the completeness of the categorisation of functions and classification of equipment interfaces, how the response time requirements are met by the PLS architecture, and why the PLS requires Heating, Ventilation and Air Conditioning (HVAC) to be operational in order to fulfil its functions.

42. The responses to the queries provided the requested clarifications and Ref. 3 was updated to incorporate the responses (in Ref. 48). Westinghouse confirmed that the detailed categorisation of PLS functions and classification of interfaces including justification of their adequacy will be performed post-GDA (in accordance with existing Step 4 assessment findings AF-AP1000-FS-01, 02 and 03). The Westinghouse resolution plan stated that Westinghouse would "identify and justify all systems connected directly or indirectly to the DCIS". However, the GDA issue does not require performance of this activity during GDA, therefore, the position reached is acceptable for closure of the GDA issue.

43. The justification of connected systems shall:

- address the safety relevance of all interfaces (direct and indirect);

- address all tools such as those used to configure and maintain the system (see discussion on tools below);
- provide an indication of data sent or received from different category systems;
- demonstrate the achievement of the safety of each system (for example, that the response to data transmission corruption is appropriate).

I have included the requirement to undertake the justification of all connected systems and interfaces under assessment findings CP-AF-AP1000-CI-007 and CP-AF-AP1000-CI-008 below.

44. The demonstration of how the PLS meets its response time requirements is contained in the *AP1000 Plant Control System Thread Path Analysis Report* (Ref. 28) (requested under RQ-AP1000-1743). I reviewed Ref. 28 and found it identifies the response time requirements (for example, that MCR displays are updated within three seconds of scan time). The analysis presents models that identify the data flow paths from sensor inputs to actuators/displays, and the worst-case time delay for system elements (for example, input/output cards) involved in the thread path. The thread path analysis for PLS and DDS functions demonstrates that execution time requirements are fulfilled (for example, as summarised in Ref. 28, Table 4-1). I judge that Ref. 28 provides an adequate PLS/DDS response time analysis.

45. In response to RQ-AP1000-1701 (query 18), Westinghouse clarified that the PLS is not directly credited for primary mitigation of any design basis fault or diverse mitigation of any frequent faults. The *AP1000 Pre-Construction Safety Report, Chapter 8 – Fault and Accident Analysis* (Ref. 57), Table 8A-4 *Support Systems for Front Line SSCs Listed in Table 8A-2* shows that PLS and HVAC are required for the normal residual heat removal system (RNS) injection function, 'RNS inject'. The HVAC is noted to be Class 2 in Table 8A-4 (that is, it aligns with the Class of the PLS) and the HVAC C&I will need to be justified accordingly. Assessment finding CP-AF-AP1000-CI-007 (see below) includes a requirement for the licensee to ensure that PLS support systems, such as HVAC, are justified to an appropriate Class.

46. In support of my assessment of Ref. 3, I sampled the following reference documents:

- AP1000 Plant Control System Reliability Analysis – APP-PLS-GR-002, Rev. 0 (Ref. 25);
- Ovation DCS Platform Reliability – WNA-AR-00039-GEN, Rev. 1 (Ref. 26) (since Ref. 25 makes use of the results of Ref. 26);
- AP1000 Plant Control System/Data Display and Processing System Requirements Specification – APP-PLS-J4-004, Rev. 6 (Ref. 27).

47. I determined that Refs. 25 and 26 present the method for and results of the Ovation platform and PLS hardware reliability analyses used to determine the hardware reliability. The reliability analyses include use of a Reliability Block Diagram (RBD) approach, Failures Modes and Effects Analysis (FMEA) and a commercially-available analysis tool. The Ovation platform components reliability analysis (Ref. 26) provides an adequate basis for determining the reliability of the Ovation modules. The results of the Ovation components reliability analysis are used in the PLS reliability analysis (Ref. 25).

48. I found that the reliability analysis approach adopted by Westinghouse considers all failures and not just dangerous failures, thereby providing conservative results. Ref. 25 compares the calculated reliability values against Westinghouse's reliability targets (for example, plant outages less than 0.01 events per year). However, I noted that the

analysis does not address CCFs; further work is required to demonstrate that Westinghouse's plant outage target is met (in particular for the CVS function as noted in Ref. 25, section 3.3.2) and the method needs to be developed to provide a PLS probability of dangerous failure per year (pdfy) value.

49. In response to my queries (for example, RQ-AP1000-1582, RQ-AP1000-1611 and RQ-AP1000-1750), Westinghouse described the method that will be used to incorporate CCF into the PLS analysis (for example, including the use of beta factors as determined following an approach outlined in IEC 61508-6), which appears reasonable. Westinghouse is to update the analysis following selection of the UK **AP1000** plants PLS components as the design is finalised post GDA. The update will provide a pdfy value and address CCFs (for example, see Ref. 48, section 5 and Appendix A). I note that Westinghouse needs to complete the demonstration that the plant outage target is met. I have captured the need for Westinghouse to complete the reliability analyses under assessment finding CP-AF-AP1000-CI-007 (see below).

50. The overall reliability value is the sum of the hardware and software values (see NS-TAST-GD-046). The value used by the PSA for PLS software CCF should be as justified by the C&I safety demonstrations, such as the standards compliance matrices (Refs. 5 and 6) (10-2 pdfy not 10-3 pdfy as stated in Ref. 3, Argument A.1.3.3.4.2). However, the ONR PSA inspector investigated the impact on plant risk of using a 10-2 pdfy value for the PLS in the PSA and confirmed that the plant risk is not unacceptable (Refs 49 and 63). In completing the reliability analyses in accordance with assessment finding CP-AF-AP1000-CI-007, Westinghouse needs to ensure that the PSA demonstrates use of the PLS software CCF value justified by the C&I safety demonstrations (10-2 pdfy) does not lead to unacceptable plant risk.

51. I reviewed the *AP1000 Plant Control System/Data Display and Processing System Requirements Specification – APP-PLS-J4-004* (Ref. 27) using relevant clauses of IEC 61513 (for example, clause 6.2.2.2.2 on application functions' requirements specifications) as the basis of my review. I also reviewed the section of Ref. 5 that provided the CAE for IEC 61513 clause 6.2.2.2.2. Ref. 27 defines the functional and design requirements for the PLS and the DDS. The document includes requirements traceability information (for example, in tabular form) that defines the source of the requirements captured therein. I found that Ref. 27 does not explicitly define the specific ranges, set-points and performance requirements. The system functional requirements documents and corresponding calculation notes define these requirements.

52. I sampled requirements documents, provided in response to RQ-AP1000-1700, relevant to the pressuriser pressure and level control function provided by the PLS (for example, *AP1000 Pressurizer Pressure Control System Functional Requirements* (Ref. 53) and calculation note *Reactor Coolant System Control Requirements* (Ref. 54)). I traced functional requirements (for example, for pressuriser spray block valves) from Ref. 27 into the relevant functional requirements document and calculation note (see Ref. 18). I am content that Ref. 27, together with the supporting documents, define the PLS requirements for the standard **AP1000** plant. Westinghouse needs to define the precise requirements for the UK **AP1000** plant during the implementation phase of the UK **AP1000** plant project following completion of the categorisation of PLS functions (see above). I have captured the need for Westinghouse to define the UK AP1000 plant requirements under assessment finding CP-AF-AP1000-CI-007 (see below).

53. Ref. 4 provides evaluation of the PLS application and related platform elements for conformance with individual SAPs from the set provided in ONR document Safety Assessment Principles for Nuclear Facilities (Ref. 15). The conformance demonstration for each SAP uses a CAE trail format. Ref. 4 either demonstrates satisfaction of the SAPs or presents CMs for any identified gaps. I found that the scope

of SAP coverage met my expectations (for example, when compared with those defined in Ref. 19). The evaluation includes application and platform CAE trails.

54. I sampled the CAE trails for a number of SAPs (for example, ESS.27, EDR.3, ERL.2 and ESR.9) and raised queries in RQ-AP1000-1706 (for example, provision of additional evidence for Ovation platform ICBMs, coverage of all elements necessary to deliver instrumentation functions, and the absence of a description of Westinghouse's quality management system). Westinghouse provided Ref. 30, an update of Ref. 4, which includes the requested additional information (for example, definition of the Ovation platform ICBMs (see below under platform assessment), clarification of the scope of the coverage of instrumentation functions, and a description of Westinghouse's quality management system). From my review of the submission, including the sampling of selected SAPs, I consider that the submission is broadly acceptable.

55. The Westinghouse resolution plan (Ref. 2) notes that Westinghouse would revise the BSC to incorporate the changes to the design and qualification documentation and provide a revised design process that is consistent with the SAPs. The GDA issue states that CMs are required to address gaps in the SAPs and standards compliance demonstrations. The revision of the BSC (Ref. 48) presents such CMs (for example, PLS-ONRSAP-GAP-038 – "Define a process to specify reliability, range, stability, response time and accuracy of instrumentation for the AP1000 UK"). Therefore, the position in relation to closure of the GDA issue is acceptable. I have included the requirement to implement the CMs under assessment finding CP-AF-AP1000-CI-007 below.

56. Of particular note is Westinghouse's approach to conformance to ESS.27, as outlined in Ref. 3, which defines the Production Excellence (PE) and ICBM legs of Westinghouse's safety case for the PLS application. The main PE elements include demonstrating conformance to key nuclear sector standards such as IEC 61513, IEC 62138 and IEC 60987 and implementing a quality management system in accordance with the ISO 9001 standard. The PLS application ICBMs include an independent review of the PE evidence, static analysis of Ovation Control Builder logic diagrams, dynamic software testing as part of the system integration testing and commissioning testing performed by the site testing organisation (independent of the system design organisation). In completing the safety case in accordance with assessment finding CP-AF-AP1000-CI-007 (see below), the licensee shall ensure the independence of those defining and undertaking the ICBMs (for example, those developing the commissioning tests as well as performing them) from the system's specifiers and developers in accordance with NS-TAST-GD-046.

57. Given the areas for improvement identified during the commercial grade survey (see below under platform assessment), I queried (RQ-AP1000-1752) the potential for Westinghouse to enhance the ICBMs by, for example, including statistical testing of the PLS alarm functions (covering both application and platform elements). Westinghouse provided Ref. 48, a revision of Ref. 3, which includes a commitment to undertake statistical testing (see Ref. 48, section 6.6.2.3.5). Following Westinghouse's commitment to enhance the ICBMs, I am content with Westinghouse's proposals for addressing ESS.27 for the PLS application.

58. I reviewed Ref. 5, the purpose of which is to demonstrate the extent of conformance to the IEC 61513 safety lifecycle for the PLS application. Ref. 5 also includes reference to platform qualification evidence such as the commercial grade survey (Ref. 13) in response to IEC 61513 clauses (for example, clause 6.2.2.7) that are relevant to the Ovation platform. My review of Ref. 5 addressed both application and platform aspects.

59. Westinghouse's approach to demonstrating conformance to the IEC 61513 safety lifecycle is based on a tabular approach that provides CAE trails for 'shall' clauses and selected objectives clauses (as confirmed in the response to RQ-AP1000-1594 query 2). The IEC 61513 conformance demonstration contained in Ref. 5 addresses the lowest level of IEC 61513 sub-clauses and covers all 'shall' clauses of IEC 61513 relevant to the PLS (sections 6 to 8). Ref. 5 highlights the gaps in conformance to IEC 61513 and defines the CMs for application during the UK **AP1000** plants PLS development post-GDA. Ref. 48, section 5.2 also identifies and section 4.3 discusses the gaps and CMs.

60. I raised a number of queries in RQ-AP1000-1720 following sampling of selected IEC 61513 clause conformance statements (for example, approach to incorporation of Category C safety functions and absence of reference to reliability analyses). Westinghouse addressed my queries in the RQ response and Ref. 50, an update of Ref. 5. For example, Westinghouse confirmed they would implement Category C functions in line with the higher Category B requirements and provided references to reliability analyses. Ref. 5 does not address all 'should' and 'may' clauses and statements from IEC 61513. I raised RQ-AP1000-1707 asking Westinghouse to address all standards' 'should' and 'may' clauses/statements in the standards conformance/compliance documents for all C&I GDA Issues (for example, by providing compensating measures for gaps). I also asked Westinghouse to provide a full justification of its position if they did not believe it was reasonably practicable to address fully the relevant standards. In response to RQ-AP1000-1707, Westinghouse confirmed it would complete the compliance assessment to address 'should' and 'may' statements post-GDA (that is, as part of addressing existing assessment finding AF-AP1000-CI-005 (see Ref. 17)).

61. I found that Refs. 6 and 7 provide the UK **AP1000** plant PLS application compliance assessments for the IEC 62138 and 60987 standards (in support of Westinghouse's PE claim). The gaps and CMs identified in Refs. 6 and 7 are included in Ref. 3, section 5. As with Ref. 5, I noted that, for 'shall' clauses Westinghouse provided an argument, evidence trail and where needed a gap CM. I raised generic issues relating to Westinghouse's approach to standards compliance demonstrations in RQ-AP1000-1707 (see above). Westinghouse's compliance demonstrations consider 'should' and 'may' statements but do not identify gaps or CMs. For example, Westinghouse categorise 'should' statements as a 'recommendation' and if it is shown that the compliance status is 'non-compliant' a gap is not identified. In response to the RQ, Westinghouse committed to address such statements as part of the work to complete GDA assessment finding AF-AP1000-CI-005 (see Ref. 17).

62. In addition to the generic finding, I raised a number of specific queries following my review of Refs 6 and 7 (for example, in RQ-AP1000-1594 and RQ-AP1000-1479), such as identification of hardware performance requirements, scope of pre-developed software and minimisation of random hardware failures. Westinghouse provided an adequate response to my RQ queries; for example, confirming that the evidence includes hardware performance requirements and the hardware reliability analysis Ref. 25 addresses minimisation of random hardware failures. Westinghouse also confirmed that, for the PLS, only the software from Emerson and the Wind River VxWorks® Real-Time Operating System (RTOS) are considered to be pre-developed software. Westinghouse provided Ref. 33, a revision of Ref. 7 and committed to update Ref. 6 post GDA (see also AF-AP1000-CI-005 in Ref. 17).

63. I assessed the document *DCIS Important to Safety – Platform Tools Review for Ovation 3.5.1* (Ref. 32). I reviewed Ref. 32 to establish whether it supports the claims made on it in Ref. 6. Following my review, I raised a number of queries in RQ-AP1000-1744. In response, Westinghouse confirmed that outputs from all tools used to produce software (for example, Plant Wide Database, Application Capture Tool, Control Builder Automation Tool, Developer Studio and Control Builder) are verified using specific

verification tests and identified the **AP1000** plant's test procedures. The Engineer Workstation, which is part of the DDS, contains the software tools (for example, Developer Studio) for the Ovation platform used by plant personnel to configure and maintain the system. Westinghouse explained the tool configuration controls (for example, restriction of access to authorised users) that mitigate the risk of inadvertent updates, the process for managing tool faults and features to detect data corruption. Westinghouse's response broadly confirms that Ref. 32 supports the claims made on it in Ref. 6.

64. My review confirmed that, for the PLS application, the topics and elements of a BSC as outlined in the GDA issue and ONR GDA Issues Closure Guidance Document (Ref. 19) are adequately addressed by the BSC, Ref. 48 and key supporting submissions (Refs. 30, 50, 6 and 33). Ref. 48 identifies that IEC 61513 is used to implement the PLS application safety life cycle, and IEC 62138 and IEC 60987 for the application PE demonstration. Ref. 48 draws on a SAP compliance assessment (Ref. 30), which includes all relevant SAPs and defines the PE and ICBM activities. Ref 48 also addresses Step 4 TOs. In addition, the ALARP assessment identifies relevant good practice applicable to PLS development, reliability assessments of the PLS have been performed and the PSA shows the plant risk is not sensitive to changes in PLS reliability.

65. Following assessment of Westinghouse's submissions in response to GDA issue action GI-AP1000-C&I-07.A2 on provision of a BSC that includes a justification of the suitability of the PLS application at Class 2 (control), I am content that the BSC (Ref. 48), together with the supporting submissions, adequately address GDA issue action GI-AP1000-CI-07.A2 for the PLS application. I have raised an assessment finding below to capture those matters arising from my assessment that need to be addressed during the implementation of the PLS post GDA.

> GDA Assessment Finding: **CP-AF-AP1000-CI-007 –** The Licensee shall fully develop the safety case outlined in the PLS BSC, including use of the Ovation platform, and implement the BSC safety plan. This shall include but not be limited to:
>
> - Implement the Compensating Measures including those in the SAP and standards compliance matrices. This shall incorporate all clauses and all 'should' and 'may' statements within clauses.
> - Justify all PLS interfaces and tools, and complete the UK AP1000 plant's requirements definition following completion of the UK AP1000 plant's categorisation and classification activities.
> - Justify PLS support systems to an appropriate Class (Class 2 or higher). This should include HVAC systems.
> - Ensure that the PLS reliability analyses address CCF, and demonstrate that the UK reliability and outage targets are met. Ensure that the PSA applies a PLS software CCF value that is justified by the C&I safety analysis.

For further guidance on the completion of the PLS safety cases see Technical Observations CI-07-TO2-2.2.3.2.3-1 and 2, CI-07-TO2-2.4.2.3-1 and 2, CI-07-TO2-2.4.2.5-1, CI-07-TO2-2.4.2.7-1, 2, 5, 6 and 8 to 14, CI-07-TO2-2.4.2.8-2 to 4, CI-07-TO2-2.4.2.9-1, 3 and 4, CI-07-TO2-2.4.2.12-6, CI-07-TO2-2.4.3.1-1 and 2, CI-07-TO2-2.4.3.2-1 to 4 and CI-07-TO2-2.4.3.3-1 in Ref. 18.

4.2.2.2 DDS Application Assessment

66. This section contains my assessment of Westinghouse's response to GDA issue action GI-AP1000-C&I-07.A2 for the DDS application. Section 4.2.2 above provides an overview of the structure and content of Ref. 8. The overall objective of Ref. 8 is to provide an adequate safety demonstration for functions that support the Operation and Control Centres System manual control of PLS functions and communication of plant data (for example, operator alarms). The DDS includes the Engineering Workstations used by plant operators to configure and maintain the PLS. Following review of Ref. 8, I raised a number of queries in RQ-AP1000-1764. For example, Westinghouse to identify all interfaces, clarify where one way interfaces are required to ensure independence of systems, confirm that higher Class systems do not rely on DDS data or justify why this is acceptable, and justify the acceptability of performing PLS modifications from the DDS.

67. The response to RQ-AP1000-1764 and Ref. 45, a revision of Ref. 8, addressed the topics raised and provided the requested clarifications. Westinghouse clarified that the architecture figures provided in Ref. 45 (that is, figures 1-1, 3-1 and 3-2) are representative of the DDS architecture for the standard **AP1000** plant design. Details of the chosen architecture of the UK **AP1000** plant's DDS will be provided during the detailed design phase following confirmation of the Class of all systems (in accordance with the established assessment findings AF-AP1000-FS-01, 02 and 03). This will include providing details of the independence needs for systems of differing Class.

68. Westinghouse's response (for example, see Ref. 45, section 4.4) noted it will confirm the control functionality of the systems of different Class is achieved without the use of data managed by the DDS using, for example, the guidance presented in the document *Study into use of PLCs in Low-SIL systems: Safety Justification* (Ref. 64). Westinghouse is to produce a Class 3 Communications Safety Justification report that will include the safety relevance of each interface, an indication of data sent or received from different category systems and a justification of the safety of each system (for example, the response to data transmission corruption is appropriate).

69. Westinghouse confirmed that software upgrades to the PLS are made from the DDS and outlined (see Ref. 45) the various checks and balances available to detect anomalies (for example, consistency check, reconcile and load diagnostics). Westinghouse also note that Ref. 45 contains gap DDS-ONRSAPS-GAP-001, that requires the performance of an additional analysis to verify any failure in a lower Class item will not propagate to an item of a higher Class. However, the changes to Ref. 8, as presented in Ref. 45, also identify that the system can be modified on-line at power. The licensee must provide an adequate operational phase change control process that does not allow changes on-line at power (unless the licensee provides a rigorous justification for any such changes). I have included this expectation under assessment finding CP-AF-AP1000-CI-008 below.

70. The PE elements for the DDS application to be developed by Westinghouse are: compliance to the IEC 61513 safety lifecycle (sections 6, 7 and 8); conformance to relevant ONR SAPs and the IEC 62138 standard; and implementation of Westinghouse's ISO 9001 compliant QMS. The ICBMs for the DDS application development are: an independent review of the **AP1000** plant's DDS PE evidence documentation; commissioning tests; and provision of a schedule for in-service examination, inspection, maintenance and testing activities.

71. I queried (RQ-AP1000-1764) the reasonable practicability of Westinghouse providing further ICBMs for the DDS application and platform software. In response, Westinghouse clarified its intention to carry out dynamic testing on the PLS using simulation models to represent the plant components under control and use of DDS workstations and displays for viewing the DDS alarms. Westinghouse also confirmed (Ref. 52) that the use of DDS equipment during PLS statistical testing provides an additional DDS ICBM (that is, an evaluation of the DDS software exercised as part of

the PLS statistical test such as the Base Alarm System). I am content that the ICBMs proposed by Westinghouse are adequate (for example, in accordance with the *PLC Best Practice Guidelines* report (Ref. 29)).

72. Ref. 9 evaluates the DDS lifecycle for conformance with individual SAPs from the set contained in Ref. 15. It provides a demonstration for each SAP, in a CAE trail format, that the SAPs are satisfied, and provides supporting evidence for Ref. 8. I found that the scope of SAP coverage met my expectations. I noted during my review of Ref. 8 that the list of SAPs used for the DDS safety justification (Table 5-3) covers all of the relevant C&I SAPs listed in Ref. 19.

73. I sampled the CAE trails for SAPs ESS.27, ESR.5, ESR.9, ESR.10, EDR.2, EDR.3 and EMT.7. Following my SAPs review, I raised a number of queries in RQ-AP1000-1764. For example, I asked Westinghouse to:

- clarify the approach to coverage of lower-tier IEC standards such as those identified in IEC 61513;
- clarify its use of LowSIL PC guidance for configuring and justifying the DDS Commercial Off-The-Shelf (COTS) equipment in the specific DDS application;
- clarify its approach to software/firmware contained in DDS components;
- provide identification of Westinghouse's quality management system as applicable to DDS application development in the CAE trails;
- provide substantiation of the reliability claims.

Note RQ-AP1000-1764 included queries on both Ref. 8 and Ref. 9. LowSIL PC is an approach developed by the UK nuclear industry for justification of commercial PC equipment for use in modest-integrity safety-related applications (see Ref. 58).

74. In response to RQ-AP1000-1764 Westinghouse outlined its approach to the use of the lower-tier standards and included an IEC 61513 normative references table in section 5.2 of Ref. 45. The response confirmed that DDS Class 3 equipment will meet the requirements of Ref. 37 and *Guidelines for the Selection of Class 3 Hardware Device*" (Ref. 41). (See comments on Refs. 37 and 41 in section 4.2.2.3 below.) Westinghouse stated that the guidelines used for the assessment of the DDS Application Server software include use of IEC 62138 standard's clauses (see *Software Assessment for the Application Server* (Ref. 43)).

75. Westinghouse explained that the document *Guidelines for a Class 3 Workstation with Windows® Server 2012 R2* (Ref. 55) provides the guidance for configuration of Class 3 workstations. Westinghouse used the LowSIL PC document *Guidelines for Using Non Safety Justified Components in Systems Having a Modest Integrity Target (LowSIL): Annex B – Guidance specific to a commodity personal computer running Microsoft® Windows® 7* (Ref. 56) in support of the development of its guidelines. Westinghouse's response adequately addressed the need to configure appropriately the Windows® workstations. (See section 4.2.2.3 below for a discussion on the use of the LowSIL PC approach for the identification and mitigation of risks associated with the use of such COTS equipment.)

76. With regard to COTS software/firmware, Westinghouse explained that the UK **AP1000** plant's DDS COTS equipment would be different to that currently defined in the document *Platform Definition for Ovation 3.5.1* (Ref. 44). Westinghouse confirmed that it will provide, following equipment selection for the UK DDS, a justification for DDS COTS equipment firmware (as recorded in the CM, CM.1.3 for ESR.5 in the update to Ref. 9 (Ref. 42)). I have captured the need for Westinghouse to produce the

justification of DDS COTS equipment firmware in accordance with an appropriate standard such as IEC 62138 under assessment finding CP-AF-AP1000-CI-008 below.

77. Westinghouse confirmed that a quantitative reliability analysis would be prepared for the UK DDS (for example, see gap DDS-ONRSAPS-GAP-010 in Ref. 45). Westinghouse also included identification of Westinghouse's quality management system, as applicable to DDS application development, in the CAE trail for SAP ESS.27 (for example, Argument A.1.2) in Ref. 42.

78. I reviewed Westinghouse's DDS IEC 61513 CAE submission Ref. 10. The purpose of Ref. 10 is to demonstrate the extent of conformance with IEC 61513 for the DDS application. I found that the approach was similar to that for the PLS. For example, reference is made to the commercial grade survey (Ref. 13) in response to IEC 61513 clauses such as clause 6.2.2.7, and the CAE trail only includes 'shall' clauses, as well as certain objectives clauses. As a result, my review of Ref. 10 addressed both application and platform IEC 61513 clauses.

79. The compliance assessment to address the omitted IEC 61513 clauses will be completed post GDA as part of addressing existing assessment finding AF-AP1000-CI-005 (see Ref. 17). Westinghouse highlighted the gaps in conformance to the standard and defined CMs for implementation during the UK **AP1000** plant's DDS development. Ref. 8 identifies the gaps and CMs in section 5.2, and discusses closure of the gaps in section 4.3 (for example, implementation of the safety lifecycle includes production of additional evidence documents). The CAE trails address the lowest level of IEC 61513 sub-clauses (for example, clause 6.2.4.2.2 a) point1).

80. I undertook a review of selected Ref. 10 CAE trails. My DDS BSC review informed the selection of clauses for sampling. I sampled clauses relating to interface and architecture requirements, component qualification, test procedures and test records. I raised a number of queries in RQ-AP1000-1770 (for example, Westinghouse to clarify the coverage of COTS components in the CAE trails, arrangements for configuration control of data and approach to justifying firmware in components). In response, Westinghouse clarified how it addresses COTS components, noted a gap and CM requiring improvements to the DDS System Specification for selection of COTS components and referenced the applicable guidance. Westinghouse confirmed that it treats firmware in components as software (see above comments on firmware and reference to CM.1.3). Westinghouse stated that they consider configuration data to be software and software configuration management procedures apply to configuration data. Additional text has been added to the revision of Ref. 10, (i.e. Ref. 46), to capture the responses to the RQ (for example, sub-claim SC.1.11.3 was modified to reference the configuration management procedure).

81. Ref. 11 provides an IEC 62138 compliance assessment for the DDS application software (in support of Westinghouse's production excellence claim). Ref. 8 includes the gaps and CMs identified in Ref. 11, section 5.3 and discusses closure of the gaps in section 4.3. For 'shall' clauses within the standard, Westinghouse provided an argument, evidence trail and as appropriate a gap CM. The work to complete GDA assessment finding AF-AP1000-CI-005 (see Ref. 17) will address Gaps and CMs for 'should' and 'may' clauses and statements.

82. I raised a number of queries in RQ-AP1000-1461, following my review of Ref. 11, which included sampling of the CAE trails for selected clauses (for example, relating to requirements specification, design and verification activities). I also asked Westinghouse to address missing gap CM descriptions, and improve the CAE trail argumentation and clarity of the links to evidence. Westinghouse's response to the RQ is contained in a revision of Ref. 11 (Ref. 35). I reviewed Ref. 35 and found the document revision had addressed my queries (for example, CMs are identified and

included in the DDS BSC Ref. 8, section 5.3 and the argumentation clearly defines the link between the claim and evidence).

83. The Westinghouse resolution plan for GI-AP1000-CI-06 and GI-AP1000-CI-07 (Ref. 2) identifies Westinghouse document *Equipment Qualification Summary Report for Data Display System for Use in the AP1000 Plant* (Ref. 36) as a submission relevant to the DDS application. Ref. 36 demonstrates that the DDS cabinets are qualified in accordance with the **AP1000** plant's EQ methodology. It is noted that the cabinets used by the PLS, while demonstrated to meet US requirements, still require to be demonstrated to meet UK expectations (for Class 2 and 3 requirements) by the licensee. The DDS and PLS BSC safety plans include CMs in relation to conformance to qualification expectations as outlined in SAPs and IEC 61513 (for example, DDS-ONRSAPS-GAP-024, DDS-IEC61513-GAP-114 and PLS-IEC61513-GAP-106).

84. I confirmed that for the DDS the topics and elements of a BSC as outlined in the GDA issue and ONR GDA Issues Closure Guidance Document (Ref. 19) are adequately addressed by the BSC (Ref. 45) and key supporting submissions (Refs. 42, 46 and 35). Ref. 45 identifies the use of IEC 61513 to define the DDS safety life cycle and IEC 62138 for the production excellence demonstration. The BSC draws on a SAP compliance assessment (Ref. 42), which includes all relevant SAPs and addresses Step 4 TOs. In addition, the BSC ALARP assessment identifies relevant good practice applicable to DDS development and use of risk analysis tools to inform the design.

85. Following assessment of Westinghouse's submissions in response to GDA issue action GI-AP1000-C&I-07.A2 on provision of a BSC that includes a justification of the suitability of the DDS application at Class 3, I am content that the BSC (Ref. 45), together with the supporting submissions, adequately address GDA issue action GI-AP1000-CI-07.A2 for the DDS application. I have raised an assessment finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the DDS using the Ovation platform.

> GDA Assessment Finding: **CP-AF-AP1000-CI-008** – The Licensee shall fully develop the safety case outlined in the DDS BSC and implement the BSC safety plan. This shall include but not be limited to:
>
> - Justify the final DDS design including use of the Ovation platform in the safety case.
> - Implement the Compensating Measures including those in the SAP and standards compliance matrices. This shall incorporate all clauses and all 'should' and 'may' statements within clauses.
> - Justify all DDS COTS firmware and software identified during the detail design phase.
> - Justify all DDS interfaces (for example, data sent to higher class systems) following completion of the UK **AP1000** plant's categorisation and classification activities.
> - Implement an operational phase change control process that prevents changes on-line at power unless a rigorous justification for any such changes is made.

For further guidance on the completion of the DDS safety case, see Technical Observations CI-07-TO2-2.4.2.2-1 to 3, CI-07-TO2-2.4.2.9-2, CI-07-TO2-2.4.2.10-1 to 14 and CI-07-TO2-2.4.2.11-1 to 3 in Ref. 18.

4.2.2.3 Platform Assessment

86. This section provides my assessment of the PLS and DDS platform components. The platform comprises PLS Class 2 and DDS Class 3 components. The PLS Class 2 Emerson components include items such as the Controller and I/O cards, and COTS components such as the VxWorks® operating system. The DDS Class 3 equipment includes COTS components supplied by various manufacturers, such as servers, workstations, network switches and third-party software. Ref. 44 defines the platform components. The PLS diversity analyses to be undertaken in response to Step 4 assessment finding AF-AP1000-CI-036 will need to include consideration of all components identified in Ref. 44; for example, all complex components such as Altera FPGAs (see assessment finding CP-AF-AP1000-CI-009 below).

87. The PLS Class 2 platform PE activities and ICBMs are defined in Ref. 3. The commercial dedication survey, as reported in Ref. 13, provides the major platform PE demonstration for both Class 2 and 3 components. I confirmed that the survey used appropriate nuclear sector standards as its basis; see comments below in relation to the DCIS Commercial Dedication Plan (Ref. 12). The PLS SAP and IEC 61513 CAE submissions (Refs. 4 and 5) also address platform elements (see comments on review of Refs. 4 and 5 in section 4.2.2.1 above).

88. The ICBMs applicable to the PLS Class 2 platform are:

- independent review of PE;
- Operational Experience (OPEX) review;
- supplier pedigree assessment;
- Quality Assurance certification for platform suppliers;
- review of independent certifications for platform suppliers;
- component type testing, analyses of the previous environmental type test reports for the Class 2 parts of the Ovation platform;
- programming tools review;
- review of manufacturer's development process, Westinghouse shall facilitate the licensee's inspection of the assembled equipment;
- hardware reliability analysis, including FMEA for the PLS Ovation platform hardware components.

89. Following my review of Ref. 3, I raised a number of platform-related queries in RQ-AP1000-1701; for example, justification of communications modules (HART, Profibus and Modbus) and the use of static analysis as a platform ICBM.

90. Westinghouse confirmed that it will evaluate the HART, Profibus and Modbus modules using the commercial dedication process outlined in Ref. 12. Westinghouse will provide an assessment of the communications protocols following selection of the UK **AP1000** plant's Ovation version. The assessment will be in accordance with the *PLC Best Practice Guidelines* report (Ref. 29). I raised further queries in relation to the use of Ref. 29 (for example, usage base of the protocols and further details of the assessment approach) in RQ-AP1000-1775. Westinghouse's response identified the large user base of the proposed protocols. In addition, Westinghouse is to provide a documented history of satisfactory operation in Westinghouse applications, conduct transmission and response time system tests, confirm that the communications systems do not compromise the safety functions, and provide any necessary CMs (for example, tests to demonstrate correct functionality and error handling). Westinghouse

updated Ref. 3 to include the requested clarifications (for example, see Ref. 48, section 5.5 and Appendix B).

91. Westinghouse will undertake static analysis of the Ovation Controller source code (as outlined in WNA-AR-00535-GEN Rev A – *Distributed Control & Information Systems, Systems Important to Safety Software Static Analysis Review for the Ovation 3.6 Controller Software* (Ref. 24)). I requested a number of clarifications (RQ-AP-1000-1777) in relation to the proposed static analysis such as whether the static analysis is a PE or ICBM measure, how it contributes to the safety case, and the Ovation version to be analysed. Westinghouse clarified that the static analysis is an ICBM, the analysis will be performed on the version of Ovation Controller to be used for the UK **AP1000** plant project, and Ref. 24 should be considered as an example of the analysis to be performed. The static analysis document provided for the Ovation Controller software will contain a codes and standards applicability section, discussing how the document addresses IEC 62138, and provide tool justification. Westinghouse updated Ref. 3 to include the requested clarifications (see Ref. 48, section 6.6.2.2.9).

92. In support of my review of Ref. 6 (see above under PLS application), I assessed the document entitled *Ovation Platform Operational Experience (OPEX-P) Review for Ovation 3.5.1* (Ref. 31). I undertook the review of Ref. 31 to gain an understanding of Westinghouse's approach to OPEX demonstrations and to determine if any significant shortfalls exist. In the response to RQ-AP1000-1594, Westinghouse stated "at the point in the design lifecycle when the range of PLS hardware and software versions associated with the UK **AP1000** has been identified a review of appropriate OPEX will take place". In response to RQ-AP1000-1755, Westinghouse explained that Ref. 31 does not provide a clause-by-clause demonstration of compliance to the requirements of IEC 61508-2 Clause 7.4.10 (that is, it does not support a proven-in-use argument for the Ovation platform). Westinghouse considers that the document, by reviewing the reported platform errors and their disposition, is an example of relevant good practice. Westinghouse also noted the additional CMs identified following ONR inspection of Emerson (see below), which includes PLS statistical testing (500 statistically-valid tests of the alarm functions).

93. Ref. 8 contains Westinghouse's definition of PE and ICBMs for the DDS Class 3 platform. The commercial dedication survey (Ref. 13), and DDS SAP and IEC 61513 CAEs, Refs. 9 and 10 (see reviews of Refs. 9 and 10 in section 4.2.2.2) provide the DDS platform PE argument. The DDS Class 3 platform ICBMs are: an independent review of DDS PE, a platform OPEX review, the provision of quality assurance certificates for the relevant manufacturers and suppliers of the DDS Ovation platform and/or platform components, and hardware reliability analysis/FMEA for the DDS Ovation platform hardware components.

94. In support of and prior to the commercial dedication survey, Westinghouse produced a DCIS Commercial Dedication Plan (Ref. 12). Ref. 12 describes the process for qualifying the commercial grade Ovation platform for implementation of important-to-safety Category B and C functions (as defined in IEC 61226). This requires a demonstration that the platform components meet the requirements of Class 2 and 3 IEC nuclear sector standards. Ref. 12 draws on IEC nuclear sector standards IEC 61513, IEC 60987 and IEC 62138 for identification of relevant survey criteria. Following my review of Ref. 12, I raised a number of queries in RQ-AP1000-1382 and RQ-AP1000-1532, such as for Westinghouse to clarify the approach to demonstrating satisfaction of each clause of the standards, how Hardware Description Language (HDL) Programmed Devices (HPD) would be assessed, and the use of current LowSIL PC approach documents.

95. The response to the RQs, the revision of Ref. 12 (Ref 37) and the Commercial Grade Survey Specification (Ref. 38) provided the requested clarifications. For example, Ref. 37 includes clarification of the standards' clauses within the scope of the assessment,

discusses their applicability and includes reference to IEC 61508-2 as the basis for assessing HPDs. Ref. 38 includes detailed clause-by-clause compliance tables for each of the standards' clauses within the scope of the commercial grade survey.

96. The response to RQ-AP1000-1382 outlined the LowSIL PC assessment documents within the scope of the survey. However, Westinghouse indicated its intention to remove the description of the LowSIL PC approach from the commercial dedication plan (Ref. 37) and include it in Ref. 45. Westinghouse undertook this course of action as the LowSIL PC approach is specific to the UK **AP1000** plant project and the commercial grade survey addresses generic aspects (that is, those applicable to all **AP1000** plant projects using the Ovation platform). I confirmed that Ref. 45 identifies the LowSIL PC approach (as support to the generation of Westinghouse's guidelines for configuration of Class 3 workstations (see Ref. 48, section 6.6.1)).

97. The LowSIL PC approach (see Ref. 58) also provides guidelines for the identification and mitigation of risks associated with the use of such equipment that the licensee will need to consider. The licensee shall review relevant research into the use of Class 3 COTS equipment, such as LowSIL PC, and ensure that the approach adopted for the justification of COTS equipment is fully in alignment with recognised good practice and guidance at the time of project implementation (for example, for lockdown of PCs, and identification and mitigation of risks). I have included the need for the licensee to ensure that the approach adopted for the justification of Class 3 COTS equipment meets recognised good practice and guidance (for example, LowSIL PC guidance) under assessment finding CP-AF-AP1000-CI-009 below.

98. I asked Westinghouse to clarify the standards applicable to the DDS Class 3 hardware (RQ-AP1000-1764). In response, Westinghouse identified Ref. 41 as relevant guidance for its assessment of the design and quality assurance standards applied by suppliers of Class 3 equipment. Ref. 41 aligns Class 3 with IEC 61508-2 SIL 1 requirements and provides, among others, guidance on the content of equipment specifications and supplier assessment criteria (for example, covering design, manufacturing processes and quality assurance). While Ref. 41 does not provide a rigorous compliance demonstration for Class 3 hardware against a standard such as IEC 61508-2, it does note that the criteria were adapted from procedures and standards such as IEC 61508-2 (that is, consideration of SIL 1 measures and recommendations). I have included a requirement for the licensee to produce a compliance demonstration, using a suitable standard such as IEC 61508-2, for the Class 3 hardware selected during the detail design phase under assessment finding CP-AF-AP1000-CI-009 below.

99. Following execution of the commercial grade survey (in accordance with Refs. 37 and 38), Westinghouse submitted the Commercial Dedication Report for the Ovation 3.5.1 Platform (Ref. 13). I reviewed the submission and issued RQ-AP1000-1533 and RQ-AP1000-1658 to request clarification of various points. For example, I asked Westinghouse to clarify the claim made in relation to the development processes (for example, full compliance to the standards), revision numbers of components addressed, timeframe for completing the CM, approach to development and testing of HPDs and precise identification of evidence.

100. Westinghouse's response to the RQs and revision of Ref. 13 (Ref. 39) provided the requested clarifications. For example, Westinghouse explained that the overall claim is that the Emerson processes assessed in Ref. 39 are partially compliant to the IEC nuclear standards with gaps and CMs identified. Westinghouse's assessment of Emerson covered the lifecycle processes for all UK **AP1000** plant components and third-party products. Ref. 39 provided a more detailed assessment of HPDs, improved referencing of evidence and hardware revision numbers. Westinghouse confirmed the timeframe for completing the CMs and clarified the software versions assessed.

101. I undertook an inspection at an Emerson UK facility to independently review the Emerson Ovation platform processes and further my assessment of Ref. 39. I arranged the Ovation platform inspection in accordance with an agreed process for access to Emerson information (Ref. 22). I transmitted my sampling strategy (Ref. 23) to Westinghouse prior to the inspection.

102. The inspection looked at two threads in order to provide diversity in the approach. I selected a number of hardware and software modules for sampling and reviewed the development lifecycle of these modules. In addition, I selected a number of clauses within Ref. 39 (for IEC 61513, IEC 60987 and IEC 62138) and then reviewed the evidence to gain confidence in the Westinghouse position against these clauses.

103. I found a significant number of areas for improvement during the inspection. From a sample of 43 clauses from Ref. 39, I found the response by Westinghouse for 20 of them to be at variance with my findings. In all cases, I raised this with Westinghouse during the inspection. This is a high percentage and reduced my confidence in Ref. 39 and its conclusions. I gave feedback to Westinghouse and Emerson on the key findings of the inspection at the close-out meeting. I documented my inspection findings in *AP1000 – C&I Emerson Audit – 18th, 19th and 20th October 2016 – Note for the Record* (Ref. 61) and *Emerson DCIS Inspection Report* (Ref. 62). I issued RQ-AP1000-1752, which requested that Westinghouse provide a response to the inspection findings (that is, for each individual finding and consideration of the impact of the total findings on Westinghouse's Ovation platform justification). The main areas for improvement identified by the inspection cover:

- quality assurance arrangements and project quality plan;
- configuration and change management;
- traceability (for example, from user requirements to code) and documentation (for example, shortfall in design documentation);
- approvals (of all artefacts) and design reviews;
- roles, responsibilities and competence records;
- process and procedures;
- independence of designers, coders and verification and validation staff;
- verification and validation;
- lifecycle planning documents;
- third-party software (for example, PE evidence for VxWorks®).

104. Westinghouse responded to the inspection findings contained in RQ-AP1000-1752 by:

- committing to an independent Westinghouse inspection of the specific modules (software and hardware) to be used for the UK AP1000 plant application;
- committing to update Ref. 39 following the independent Westinghouse inspection and implementation of CMs;
- specifying the CM requirements, in relation to Emerson's processes, procedures and quality assurance arrangements, and providing them to Emerson for their consideration;

- adding a PLS statistical testing ICBM and enhancing the dynamic testing ICBM to include an evaluation of DDS software.

105. With regard to the independent inspection, Westinghouse explained its intention to target the CMs to the precise gaps (that is, the CMs will not be generic). In relation to any missing test records, the CM will include testing at the module level that includes consideration of code and branch coverage. The CM requirements that Westinghouse has asked Emerson to consider include, for example:

- instigating product-specific quality and configuration management plans;
- providing traceability within a document back to its previous development stage;
- undertaking testing of components purchased (for example, in the manufacturing process on a sample of resistors and capacitors before fitting them to boards);
- improving validation processes and specifically testing;
- improving processes to manage failed tests;
- vendor recommendations already identified in Ref. 39, section 2.3 (for example, creating software release records defining constituent elements and version numbers, producing a security plan and implementing an independent review of validation procedures).

106. Westinghouse confirmed the feasibility of addressing these CMs with the support of Emerson (Ref. 51).

107. Following the inspection, I also raised further queries on Ref. 39 in RQ-AP1000-1776 (for example, Westinghouse to clarify the extent of white box testing, testing of hardware module interfaces and approach to justifying DDS COTS software). Westinghouse clarified that Emerson undertakes some white box testing on an ad-hoc basis and depending on the results of the proposed independent inspection; Westinghouse is to request further targeted testing of the more complex functions. Westinghouse considers the black box testing to be performed, as defined in the *Commercial Dedication Instruction for Ovation 3.5.1, Controller Complementary Testing* (Ref. 14) (see comments below), to be sufficient for simple functions (for example, Boolean 'AND' and 'OR' functions). Westinghouse clarified that Ref. 14 includes the performance of tests on hardware module interfaces, and following definition of the UK **AP1000** plant's DDS COTS components in the design phase, a justification for the COTS software will be produced based on IEC 62138.

108. Westinghouse provided a satisfactory response to my queries and revised Ref. 3 (Ref. 48), Ref. 8 (Ref. 45) and Ref. 9 (Ref. 42) to include commitments contained in the responses to RQ-AP1000-1752 and RQ-AP1000-1776. For example, to undertake PLS statistical testing and tool-assisted static analysis of the Ovation Controller software (see Ref. 48, sections 6.6.2.2.9 and 6.6.2.3.5) and provide the DDS COTS software justification (Ref. 42, section 12.5).

109. I also conducted a review of Ref. 14 and the *Controller Operating System Justification for Ovation 3.5.1* (Ref. 34). Ref. 39 references these two documents as major gap CMs. The main objective of Ref. 14 is to specify controller algorithm tests as a CM for development process gaps identified in Ref. 39. The scope of the complementary tests outlined in Ref. 14 is the Ovation algorithm library as testable on a virtual and physical controller processor module. Westinghouse states that the testing supports the

qualification of the Ovation Controller platform for implementation of Category B functions.

110. I reviewed Ref. 14 and raised queries in RQ-AP1000-1609 covering, for example, the scope of the algorithms to be tested, test coverage (for example, input/output ranges, set-points, accuracy and response times) and recording of the test environment to facilitate replication of the tests. The response to RQ-AP1000-1609 and revision of Ref. 14 (Ref. 40) satisfactorily addressed the points raised and provided the requested clarifications. For example, Westinghouse clarified the scope of the tests and included a test principles section (for example, covering ranges and out of range values) in Ref. 40.

111. I found that Ref. 34 provided a justification for the use of the Wind River VxWorks®, version 6.8, RTOS in the Ovation 3.5.1 controller platform. The justification includes an OPEX review (30-year history), analysis of known problems and discussion of third-party evaluations (for example, use in NASA spacecraft). Emerson uses a substantially reduced (from the full available configuration) version of VxWorks® for the Ovation Controller; the unused features are not present in the controller. Westinghouse notes that, according to published literature, the Coverity static analysis tool was used on VxWorks® by Wind River (version 6.0 and thereafter).

112. I raised a number of queries in RQ-AP1000-1761 related to the adequacy of the OPEX review (using the guidance for a proven-in-use case as presented, for example, in IEC 61508-2). In response, Westinghouse explained that Ref. 34 was not conceived or intended to provide a clause-by-clause compliance demonstration to the requirements of IEC 61508-2 Clause 7.4.10, and it does not support a proven-in-use argument for the Ovation Controller's operating system, VxWorks®. Westinghouse has committed to undertake additional CMs such as statistical testing of the UK **AP1000** plant's PLS alarm functions. This provides coverage of VxWorks® both statistically for the alarm functions and qualitatively for other functions. The UK **AP1000** plants PLS application test programme and the dynamic testing ICBM also provide evidence of the correct operation of the VxWorks® operating system. Ref. 34 provides an outline of the pedigree of VxWorks® and describes the third-party evaluations. It also describes how Emerson has resolved VxWorks®-related problems. I am content that the case made for VxWorks® in the UK **AP1000** plant application is satisfactory.

113. Following assessment of Westinghouse's submissions in response to GDA issue action GI-AP1000-CI-06.A2, I am content that the BSCs (Refs. 45 and 48) and key platform submissions (Refs. 34, 37, 38, 39, 40 and 42) provide a reasonable basis for the justification of the Ovation platform, and that GDA issue action GI-AP1000-CI-06.A2 can be closed. The licensee will need to pay particular attention to ensuring that the significant numbers of areas for improvement in the platform justification are addressed satisfactorily (for example, by audit of Westinghouse and the platform supplier). The licensee shall confirm the definition and implementation of an appropriate set of CMs and vendor recommendations (in response to Westinghouse's commercial grade survey (Ref. 39), ONR's inspection (Refs. 61 and 62) and the proposed Westinghouse independent inspection). I have raised an assessment finding below to capture those matters arising from the assessment that need to be addressed during the implementation of the PLS and DDS using the Ovation platform.

> GDA Assessment Finding: **CP-AF-AP1000-CI-009 –** The Licensee shall complete the justification of the Ovation platform for Class 2 (PLS) and Class 3 (DDS) implementation of Category B and C functions. The justification shall include but not be limited to:
>
> - Confirmation that the platform related activities in the PLS and DDS BSC safety plans are completed.

- Demonstrate that the Class 3 hardware selected during the detail design complies with a recognised standard such as IEC 61508-2.
- Ensure the approach adopted for the justification of Class 3 COTS equipment meets recognised good practice and guidance (for example, LowSIL PC for lockdown of PCs and the identification and mitigation of risks).
- The Licensee shall implement the Compensating Measures and vendor recommendations from Westinghouse's commercial grade survey (Ref. 39), ONR's inspection (Refs. 61 and 62) and the proposed Westinghouse independent inspection.
- Ensure the PLS/PMS diversity analyses to be undertaken for AF-AP1000-CI-036 include all components identified in the Ovation platform definition, for example, components such as FPGAs etc.

For further guidance on the completion of the Ovation platform justification see Technical Observations CI-06-TO2-2.2.2.1-1 and 2, CI-06-TO2-2.2.2.3-1 to 8, CI-06-TO2-2.2.2.4-1 and 2, CI-06-TO2-2.2.3.1-1 to 4, CI-06-TO2-2.2.2.5-1, CI-06-TO2-2.2.4.3-1 to 6, CI-06-TO2-2.4.2.5-2, CI-06-TO2-2.4.2.7-3, 4, 7 and 15 to 20, CI-06-TO2-2.4.2.8-1 and CI-06-TO2-2.4.2.12-1 to 5, and 7 in Ref. 18.

4.2.3 Overall Conclusion on GDA Issues GI-AP1000-CI-06 and GI-AP-1000-CI-07

114. I am content that the safety justification presented for the UK PLS and DDS applications and platform represents an adequate position for the stage of development of the systems at the end of GDA, prior to detail design and implementation. I am satisfied that all four actions (see above) have been addressed satisfactorily and that GDA issues GI-AP1000-CI-06 and GI-AP-1000-CI-07 can be closed. I reached this conclusion as there is no significant shortfall against relevant good practice, established standards or significant failure in the technical quality of the final GDA safety cases for the PLS, DDS and Ovation platform (for example, Refs. 48 and 45). Westinghouse demonstrated, through its submissions for the PLS and DDS, that the conformance to the SAPs given in Table 1 is broadly acceptable for the current stage of the development of the systems' safety cases. The safety case will be further developed in accordance with IEC nuclear sector standards as the UK AP1000 plant's PLS and DDS design and implementation is completed post GDA. In addition, Westinghouse has shown an increased understanding of the expectations for UK safety case documentation, such as the PLS and DDS BSCs and supporting submissions.

115. I have raised assessment findings above to capture those matters arising from the assessment that need to be addressed during the development of the UK PLS and DDS post GDA. These matters include the need for Westinghouse to fully develop and implement processes that are in alignment with IEC nuclear standards for Class 2 and Class 3 equipment.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

116. 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 (for example, see assessment of SAPs CAE submissions (Refs. 4 and 9), and standards compliance submissions (Refs. 5, 6, 7 10 and 11)). I am content that Westinghouse has made satisfactory use of relevant standards, guidance and good practice.

4.4 Assessment Findings

117. During my assessment, three assessment findings were identified for a future licensee to take forward in their site-specific safety submissions. Details of these are contained above and in Annex 1.

118. 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.

119. 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;
- to resolve this matter, the level of detail of the design needs to be beyond what can reasonably be expected in GDA (for example, manufacturer/supplier input is required; or areas where the technology changes quickly, and so to avoid obsolescence of design).

5 CONCLUSIONS

120. This report presents the findings of the assessment of GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case, relating to the **AP1000** plant GDA closure phase.

121. To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the submissions provided by Westinghouse in response to GDA issues GI-AP1000-CI-06 Revision 0, Ovation Platform Adequacy of Safety Case and GI-AP1000-CI-07 Revision 0, DCIS Adequacy of Safety Case.

122. Overall, on the basis of my assessment, I am satisfied that GDA issues GI-AP1000-CI-06 and GI-AP1000-CI-07 can be closed.

6 REFERENCES

1. ONR HOW2 Guide NS-PER-GD-014 Revision 5 – Purpose and Scope of Permissioning, August 2015 – TRIM 2015/304735
2. Westinghouse UK AP1000 Generic Design Assessment Resolution Plan for GI-AP1000-C&I-06 & GI-AP1000-C&I-07 Ovation based DCIS justification for use – TRIM 2016/92087
3. United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case – UKP-PLS-GLR-001, Rev. 0 – TRIM 2016/297029
4. United Kingdom AP1000 Plant Control System (PLS) Safety Assessment Principle Compliance – UKP-PLS-GLR-002, Rev. 0 – TRIM 2016/243567
5. United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Plant Control System (PLS) – UKP-PLS-GLR-003, Rev. 0 – TRIM 2016/297033
6. United Kingdom AP1000 IEC 62138 Compliance Matrix for the Plant Control System – UKP-PLS-GL-002, Rev. 0 – TRIM 2016/158364
7. United Kingdom AP1000 IEC 60987 Compliance Matrix for the Plant Control System – UKP-PLS-GL-001, Rev. 0 – TRIM 2015/410287
8. United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case – UKP-DDS-GLR-001, Rev. 0 – TRIM 2016/297079
9. United Kingdom AP1000 Data Display and Processing System (DDS) Safety Assessment Principle Compliance – UKP-DDS-GLR-002, Rev. 0 – TRIM 2016/243561
10. United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Data Display and Processing System (DDS) – UKP-DDS-GLR-003, Rev. 0 – TRIM 2016/297086
11. United Kingdom AP1000 IEC 62138 Compliance Matrix for the Data Display System – UKP-DDS-GL-001, Rev. 0 – TRIM 2015/441959
12. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Plan – WNA-PV-00075-GEN, Rev. 0 – TRIM 2015/152150
13. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Report for the Ovation 3.5.1 Platform – WNA-VR-00464-GEN, Rev. 0 – TRIM 2015/478648
14. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Instruction – Ovation 3.5.1 Controller Complementary Testing – WNA-CD-00048-GEN, Rev. 0 – TRIM 2016/137362
15. Safety Assessment Principles for Nuclear Facilities 2014 Edition Revision 0 (www.onr.org.uk/saps/saps2014.pdf)
16. Office for Nuclear Regulation (ONR) Permissioning Inspection – Technical Assessment Guides (www.onr.org.uk/operational/tech_asst_guides/index.htm)
17. Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor – Assessment Report: ONR-GDA-AR-11-006. Revision 0 – www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf
18. Altran UK Ltd – Review of Submissions for the Closure of GDA Issue 06 & 07 Ovation Platform and PLS/DDS – Adequacy of Safety Case – S.P1641.40.TSC267.5. – TRIM 2017/41130
19. C&I GDA Issues Closure Guidance Document Rev. 0 – TRIM 2015/84414
20. C&I GDA Issues Closure Guidance Document Covering Letter – ONR-WEC-0006N – TRIM 2015/84411

21. ONR RQ Tracking Sheet – TRIM Ref 2016/383615

22. Engineering Center of Excellence – Distributed Control & Information Systems – Control of Emerson Information – WNA-IG-00650-GEN, Rev. 0 (Draft) – TRIM 2015/385763.

23. Emerson Ovation 3.5.1 Sampling Strategy and Inspection Schedule SP1641.039.ONR267.005 – TRIM 2016/380303

24. Distributed Control and Information Systems – Systems Important to Safety – Software Static Analysis Review for the Ovation 3.6 Controller Software – WNA-AR-00535-GEN, Rev. A – TRIM 2016/426569

25. AP1000 Plant Control System Reliability Analysis – APP-PLS-GR-002, Rev. 0 – TRIM 2016/99718

26. Ovation DCS Platform Reliability – WNA-AR-00039-GEN, Rev. 1 – TRIM 2015/47356

27. AP1000 Plant Control System/Data Display and Processing System Requirements Specification – APP-PLS-J4-004, Rev. 6 – TRIM 2016/319045

28. AP1000 Plant Control System Thread Path Analysis Report – APP-PLS-J7R-001, Rev. 1 – TRIM 2016/426557

29. PLC Best Practice Guidelines – CINIF, Atkins ref: 5128066-rep-01 v3.0 – TRIM 2016/425990

30. United Kingdom AP1000 Plant Control System (PLS) Safety Assessment Principle Compliance – UKP-PLS-GLR-002 Rev. 1 – TRIM 2016/470254

31. Distributed Control and Information Systems – Systems Important to Safety – Ovation Platform Operational Experience (OPEX-P) Review for Ovation 3.5.1 – WNA-AR-00520-GEN, Rev. 0 – TRIM 2016/323954

32. Distributed Control and Information Systems – Systems Important to Safety – Platform Tools Review for Ovation 3.5.1 – WNA-AR-00517-GEN, Rev. 0 – TRIM 2016/323950

33. United Kingdom AP1000 IEC 60987 Compliance Matrix for the Plant Control System – UKP-PLS-GL-001, Rev. 1 – TRIM 2016/260155

34. Distributed Control and Information Systems – Systems Important to Safety – Controller Operating System Justification for Ovation 3.5.1 – WNA-AR-00586-GEN, Rev. 0 – TRIM 2016/427539

35. United Kingdom AP1000 IEC 62138 Compliance Matrix for the Data Display System, UKP-DDS-GL-001 Rev. 1 – TRIM 2016/176113

36. Equipment Qualification Summary Report for the Data Display and Processing System for Use in the AP1000 Plant – APP-DDS-VBR-001, Rev. 1 – TRIM 2016/312585

37. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Plan – WNA-PV-00075-GEN, Rev. 1 – TRIM 2015/369188

38. Distributed Control and Information Systems – Systems Important to Safety – Commercial Grade Survey Specification – WNA-CD-00045-GEN, Rev. 1 – TRIM 2015/394766

39. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Report for the Ovation 3.5.1 Platform – WNA-VR-00464-GEN, Rev. 1 – TRIM 2016/344536

40. Distributed Control and Information Systems – Systems Important to Safety – Commercial Dedication Instruction – Ovation 3.5.1 Controller Complementary Testing – WNA-CD-00048-GEN, Rev. 1 – TRIM 2016/361679

41. Distributed Control and Information Systems – Systems Important to Safety – Guidelines for the Selection of Class 3 Hardware Devices – WNA-IG-00695-GEN, Rev. 0 – TRIM 2016/493618

42. United Kingdom AP1000 Data Display and Processing System (DDS) Safety Assessment Principle Compliance – UKP-DDS-GLR-002, Rev. 1 – TRIM 2016/497362

43. Distributed Control and Information Systems – Systems Important to Safety – Software Assessment for the Application Server Platform – WNA-AR-00613-GEN, Rev. 2 – TRIM 2016/493622

44. Distributed Control and Information Systems – Systems Important to Safety – Platform Definition for Ovation 3.5.1 – WNA-BD-00144-GEN, Rev. 2 – TRIM 2017/12094

45. United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case UKP-DDS-GLR-001, Rev. 1 – TRIM 2016/502541

46. United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Data Display and Processing System (DDS) – UKP-DDS-GLR-003, Rev. 1 – TRIM 2016/499804

47. ONR Assessment Rating Guide – TRIM 2016/118638

48. United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case – UKP-PLS-GLR-001, Rev. 1 – TRIM 2016/502539.

49. ONR PSA Team Assessment Report – Probabilistic Safety Analysis for the Westinghouse AP1000® Reactor. GDA issue GI-AP1000-PSA-01. Success Criteria (Internal Events At-Power) ONR-NR-AR-16-017 – TRIM 2016/275018

50. United Kingdom AP1000 IEC 61513 Claims, Arguments and Evidence for the Plant Control System (PLS) – UKP-PLS-GLR-003, Rev. 1 – TRIM 2016/470266

51. Response to RQ-AP1000-1752 – Westinghouse Moorside letter, Enclosure 02 – NPP_JNE_001447 – TRIM 2016/479624

52. Response to ONR on DDS Statistical Testing – Westinghouse Letter Unique Number WEC-REG-01533N – TRIM 2017/20196

53. AP1000 Pressurizer Pressure Control System Functional Requirements – APP-PLS-J1-061, Rev. 3 – TRIM 2016/409433

54. RCS Component Control Requirements – APP-RCS-M3C-100, Rev. 12 – TRIM 2016/409508

55. Distributed Control and Information Systems – Systems Important to Safety – Guidelines for a Class 3 Workstation with Windows® Server 2012 R2 – WNA-IG-00688-GEN, Rev. 0 – TRIM 2016/493630

56. Guidelines for Using Non Safety Justified Components in Systems Having a Modest Integrity Target (LowSIL): Annex B – Guidance specific to a commodity personal computer running Microsoft® Windows® 7 – D/919/43127/2 V1.0, United Kingdom Control and Information Nuclear Industry Forum (CINIF), 15 December 2015 – TRIM 2016/115448

57. AP1000 Pre-Construction Safety Report, Chapter 8 – Fault and Accident Analysis – NPP-JNE-001535 – TRIM 2017/22537

58. Guidelines for Using Non Safety Justified Components in Systems Having a Modest Integrity Target (LowSIL) – TRIM 2017/30597

59. ONR Guidance to Requesting Parties (www.onr.org.uk/new-reactors/ngn03.pdf)

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

61. AP1000 – C&I Emerson Audit – 18th, 19th and 20th October 2016 – Note for the Record – TRIM 2016/422080

62. Emerson DCIS Inspection Report – S.P1641.40.TSC267.5.1, Issue: 1.0, 31st October 2016 – TRIM 2017/64392

63. ONR PSA team communication on PLS reliability sensitivity – TRIM 2017/13257

64. Study into use of PLCs in Low-SIL systems: Safety Justification – TRIM 2017/106622

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-007	GDA Assessment Finding: **CP-AF-AP1000-CI-007 –** The Licensee shall fully develop the safety case outlined in the PLS BSC, including use of the Ovation platform, and implement the BSC safety plan. This shall include but not be limited to: • Implement the Compensating Measures including those in the SAP and standards compliance matrices. This shall incorporate all clauses and all 'should' and 'may' statements within clauses. • Justify all PLS interfaces and tools, and complete the UK AP1000 plant's requirements definition following completion of the UK AP1000 plant's categorisation and classification activities. • Justify PLS support systems to an appropriate Class (i.e. Class 2 or higher). This should include HVAC systems. • Ensure that the PLS reliability analyses address CCF, and demonstrate that the UK reliability and outage targets are met. Ensure that the PSA applies a PLS software CCF value that is justified by the C&I safety analysis. For further guidance on the completion of the PLS safety case see Technical Observations CI-07-TO2-2.2.3.2.3-1 and 2, CI-07-TO2-2.4.2.3-1 and 2, CI-07-TO2-2.4.2.5-1, CI-07-TO2-2.4.2.7-1, 2, 5, 6 and 8 to 14, CI-07-TO2-2.4.2.8-2 to 4, CI-07-TO2-2.4.2.9-1, 3 and 4, CI-07-TO2-2.4.2.12-6, CI-07-TO2-2.4.3.1-1 and 2, CI-07-TO2-2.4.3.2-1 to 4 and CI-07-TO2-2.4.3.3-1in Ref. 18.	4.2.2.1
CP-AF-AP1000-CI-008	GDA Assessment Finding: **CP-AF-AP1000-CI-008** – The Licensee shall fully develop the safety case outlined in the DDS BSC and implement the BSC safety plan. This shall include but not be limited to:	4.2.2.2

	• Justify the final DDS design including use of the Ovation platform in the safety case. • Implement the Compensating Measures including those in the SAP and standards compliance matrices. This shall incorporate all clauses and all 'should' and 'may' statements within clauses. • Justify all DDS COTS firmware and software identified during the detail design phase. • Justify all DDS interfaces (for example, data sent to higher class systems) following completion of the UK **AP1000** plant's categorisation and classification activities. • Implement an operational phase change control process that prevents changes on-line at power unless a rigorous justification for any such changes is made. For further guidance on the completion of the DDS safety case, see Technical Observations CI-07-TO2-2.4.2.2-1 to 3, CI-07-TO2-2.4.2.9-2, CI-07-TO2-2.4.2.10 -1 to 14 and CI-07-TO2-2.4.2.11-1 to 3 in Ref. 18.	
CP-AF-AP1000-CI-009	GDA Assessment Finding: **CP-AF-AP1000-CI-009** – The Licensee shall complete the justification of the Ovation platform for Class 2 (PLS) and Class 3 (DDS) implementation of Category B and C functions. The justification shall include but not be limited to: • Confirmation that the platform related activities in the PLS and DDS BSC safety plans are completed. • Demonstrate that the Class 3 hardware selected during the detail design complies with a recognised standard such as IEC 61508-2. • Ensure the approach adopted for the justification of Class 3 COTS equipment meets recognised good practice and guidance (for example, LowSIL PC for lockdown of PCs and the identification and mitigation of risks). • The Licensee shall implement the Compensating Measures and vendor	4.2.2.3

	recommendations from Westinghouse's commercial grade survey (Ref. 39), ONR's inspection (Refs 61 and 62) and the proposed Westinghouse independent inspection. • Ensure the PLS/PMS diversity analyses to be undertaken for AF-AP1000-CI-036 include all components identified in the Ovation platform definition, for example, components such as FPGAs etc. For further guidance on the completion of the Ovation platform justification see Technical Observations CI-06-TO2-2.2.2.1-1 and 2, CI-06-TO2-2.2.2.3-1 to 8, CI-06-TO2-2.2.2.4-1 and 2, CI-06-TO2-2.2.3.1-1 to 4, CI-06-TO2-2.2.2.5-1, CI-06-TO2-2.2.4.3-1 to 6, CI-06-TO2-2.4.2.5-2, CI-06-TO2-2.4.2.7-3, 4, 7 and 15 to 20, CI-06-TO2-2.4.2.8-1 and CI-06-TO2-2.4.2.12-1 to 5, and 7 in Ref. 18.	