New Reactors Programme

GDA Close-out for the AP1000 Reactor

GDA Issues GI-AP1000-CI-03 – Diversity of the DAS from the PMS and the PLS/DDS

Assessment Report: ONR-NR-AR-16-030
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

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

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses the GDA Issue GI-AP1000-CI-03.

This GDA issue arose in Step 4 due to the need for additional evidence supporting Westinghouse's claim of diversity between the secondary protection system, namely, the Diverse Actuation System (DAS) and:

- the primary protection system, namely, the Protection and Safety Monitoring System (PMS); and
- the plant control systems, namely, the Plant Control System (PLS) and the Data Display and Processing System (DDS), respectively.

The Westinghouse's GDA issue resolution plan (Ref. 6) stated that the approach to closing GI-AP1000-CI-03 was to provide two reports substantiating the diversity claims in the basis of safety cases for the individual C&I systems.

My assessment conclusion is that:

- the claim, argument and evidence approach proposed by Westinghouse provides adequate clarity in the substantiation of the diversity claims;
- the traceability between the clauses in the key diversity standards, such as IEC 62340 and NUREG 6303, and the claims in the submissions provided by Westinghouse has led to adequate coverage of the diversity issues expected in the resolution of GI-AP1000-CI-03; and
- the scope and the depth of the diversity analyses proposed by Westinghouse against GI-AP1000-CI-03 are adequate for de-risking future phases of UK **AP1000** project development.

My judgement is based on the assessment of the diversity analyses identified in the GI-AP1000-CI-03 resolution plan (Ref. 6) and the sampling of supporting documents:

- confirming how the introduction in the UK **AP1000** design of an analogue platform for the DAS minimises the risk for common cause failures with PMS, PLS and DDS that are all based on complex programmable electronics;
- providing an adequate justification of the resilience of the C&I systems against common cause failures as identified in relevant modern standards; and
- identifying adequate compensating measures to be implemented post-GDA when the UK DAS design is completed and the detailed design information for the UK **AP1000** design becomes available.

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

- ensure that diversity requirements are captured in the system specifications for the UK **AP1000** design; and
- fully develop the diversity analyses considering the detailed design information for the UK **AP1000** design.

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

In summary, I am satisfied that GDA Issue GI-AP1000-CI-03 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
CIM	Component Interface Module
CM	compensating measure
CMT	Core Makeup Tank
DAS	Diverse Actuation System
DDS	Data Display and Processing System
FPGA	field programmable gate array
GDA	Generic Design Assessment
HVAC	heating, ventilation and air conditioning
IDS	Uninterruptible Power Supply System (Class 1 power)
IEC	International Electrotechnical Commission
ONR	Office for Nuclear Regulation
PCSR	Pre-construction Safety Report
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PSR	Preliminary Safety Report
RP	requesting party
SAPs	Safety Assessment Principles
SFAIRP	So Far As Is Reasonably Practicable
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	technical support contractor
UPS	uninterruptible power supply

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 Background

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

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses GDA Issue GI-AP1000-CI-03 on the need for additional evidence supporting Westinghouse's claim of diversity between the secondary protection system and both the primary protection system and the plant control systems.

3. The related GDA Step 4 report is published on ONR's website (Ref. 56), and this provides the assessment underpinning the GDA issue. Further information on the GDA process in general is also available on ONR's website (Ref. 57).

1.2 Overview of GI-AP1000-CI-03

4. During Step 4 of the **AP1000** GDA (Ref. 1), ONR highlighted that the use of the Advanced Logic System proposed by Westinghouse for the standard **AP1000** plant secondary protection system, namely, the Diverse Actuation System (DAS), represented a challenge in the context of the diversity demonstration of the DAS against the other main C&I systems, namely:

    - the primary protection system, Class 1 Protection and Safety Monitoring System (PMS); and
    - the plant control systems, Class 2 Plant Control System (PLS) and the Class 3 Data Display and Processing System (DDS).

5. It is highlighted that, while in the standard **AP1000** plant design, the DAS is classified as non-safety (non-Class 1E according to USNRC Standard Review Plan (NUREG-0800), Branch Technical Position 7-19), the UK DAS performs Category A safety functions (Ref. 13) and is Class 2 (Ref. 12).

6. It is noted that in the standard **AP1000** plant design, the C&I systems are based on the following technology:

    - DAS: based on field programmable gate array (FPGA);
    - PMS: computer-based (Common Q platform);
    - Component Interface Module (CIM, part of the PMS): FPGA-based;
    - Blockers (part of the PMS): discrete electronics; and
    - PLS and DDS: computer-based (Ovation platform).

7. In GDA Step 4, Westinghouse made a commitment to change the technology for the DAS in the UK **AP1000** design from FPGA to a non-software-based system, namely, the 7300 series platform. Although, at a high level, Westinghouse's commitment addressed the main diversity concerns raised by ONR, the absence of an in-depth diversity analysis developed against modern standards, such as IEC 62340 (Ref. 10),

fell short of the relevant good practice for new nuclear power plant in the UK (see Ref. 3).

8. The GDA Issue GI-AP1000-CI-03 requests Westinghouse to provide a detailed diversity analysis for the DAS against the PMS and the PLS/DDS. It is noted that the safety justification of each individual C&I system is expected in the GDA closure in the form of basis of safety case as part of the resolution of:

- GI-AP1000-CI-01 and GI-AP1000-CI-02 for the DAS (see context in Ref. 1 and assessment in Ref. 60);
- GI-AP1000-CI-04, GI-AP1000-CI-08 and GI-AP1000-CI-09 for the PMS, including the CIM and the spurious actuation blocker (see context in Ref. 1 and assessment in Refs. 61,63 and 64); and
- GI-AP1000-CI-06 and GI-AP1000-CI-07 for the PLS and DDS (see context in Ref. 1 and assessment in Ref. 62).

1.3 Scope

9. The scope of this assessment is detailed in the assessment plan (Ref. 2).

10. Considering the design maturity for the C&I systems expected for GDA closure (see Ref. 1), my assessment mainly focused on:

- whether the change in technology for the DAS agreed in Step 4 GDA - from FPGA-based to discrete electronics - provides sufficient confidence regarding the diversity of the C&I systems at platform level;
- the identification of components of similar technology or types between the C&I systems and the justification of their diversity;
- the screening of shared component or path between C&I systems which could cause their simultaneous failure; and
- whether the arrangements proposed by Westinghouse for the detailed design of UK **AP1000** plant C&I systems ensure an adequate level of diversity.

11. I judge this approach proportionate because it allows the de-risking of the **AP1000** design regarding diversity issues. It also allows the identification of any compensating activities to be considered post-GDA during the development of the detailed design for the UK **AP1000** plant C&I systems. In addition, it is also in line with the expectations set out in other GDAs (see Ref. 3).

1.4 Method

12. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 4).

1.4.1 Sampling Strategy

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

14. In this GDA issue closure, Westinghouse provided the diversity analyses using a claim, argument and evidence (CAE) format. A sampling approach was taken to verify the adequacy of the evidence supporting the main claims in the submissions. Also, sampling was carried out to ensure that the interfaces between the C&I systems do not

compromise their diversity (see Section 4.2 in this report and Refs 16 and 17 for additional details).

15. The sampling approach adopted in this GDA issue closure also ensured adequate coverage of the key technical observations raised during GDA Step 4 under GI-AP1000-CI-03 (see Ref. 1: T18.TO1.01, T18.TO2.06, T18.TO2.11, T18.TO2.19, T18.TO2.21 and T18.TO2.25).

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

16. ONR's GDA Guidance to Requesting Parties (Ref. 52) states that the information required for GDA may be in the form of a Pre-Construction Safety Report (PCSR), and Technical Assessment Guide No. 051 (Ref. 53) sets out regulatory expectations for a PCSR.

17. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 54) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the **AP1000** design reference point.

18. A separate regulatory assessment report is provided, which considers the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, and therefore this report does not assess the C&I aspects of the PCSR. This assessment focused on the supporting documents and evidence specific to GDA Issue GI-AP1000-CI-03.

2.2 Standards and Criteria

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

2.2.1 Safety Assessment Principles

20. The key SAPs (Ref. 8) applied within the assessment are included within Table 1.

Table 1: List of applicable Safety Assessment Principles

SAP	Title
EDR.2	Redundancy, diversity and segregation
EDR.3	Common cause failure
ESS.7	Diversity in the detection of fault sequences
ESS.18	Failure independence
ERC.2	Shutdown systems

2.2.2 Technical Assessment Guides

21. The Technical Assessment Guides (TAGs) that have been used as part of this assessment are set out in Table 2.

Table 2: List of applicable Technical Assessment Guides

Identification	Title	Reference in this report
TAG-046	Computer-based safety systems	Ref. 9
TAG-003	Safety systems	Ref. 58

22. In the context of this GDA issue close-out, I mainly used Appendix 4 of TAG-046.

2.2.3 National and International Standards and Guidance

23. The international standards and guidance that have been used as part of this assessment are set out in Table 3.

Table 3: List of applicable standards and guidance

Identification	Title	Reference in this report
IEC 62340	Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)	Ref. 10
IEC 60709	Nuclear power plants – Instrumentation and control systems important to safety – Separation	Ref. 11
NUREG 6303	Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems	Ref. 14
Seven Party Paper	Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations	Ref. 15
IEC 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	Ref. 12
IEC 61226	Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions	Ref. 13
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	Ref. 59

24. In the context of this GDA issue close-out, I used IEC 61513 and IEC 61226 mainly for general context (such as general definitions, categorisation and classification) and for high-level clauses raising expectations for diversity between C&I systems in nuclear power plants.

2.3 Use of Technical Support Contractors

25. It is usual in GDA for ONR to use technical support contractors (TSCs); for example, to provide additional capacity to optimise the assessment process, to enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision-making etc.

26. Table 4 sets out the broad areas in which ONR utilised technical support. This support was required to provide additional capacity and enable access to independent advice and experience. The TSC 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	Review of the diversity strategy proposed by Westinghouse
Altran	Review of the diversity analysis between the DAS and the PMS
Altran	Review of the diversity analysis between the DAS and the PLS/DDS
Altran	Sampling of the evidence supporting Westinghouse claims in the main submissions

27. The TSC undertook the technical reviews under the close direction of and supervision by ONR. The regulatory judgement on the adequacy or otherwise of the **AP1000** design was made exclusively by ONR. ONR raised all Regulatory Queries (RQs, see Ref. 52) and meeting actions with Westinghouse.

28. The TSC has provided a report in Ref. 16 that addresses the scope of work listed above. The TSC also reviewed responses to RQs and meeting actions placed on Westinghouse. The TSC report in Ref. 17 includes a summary statement of the results of its work and findings (called Technical Observations or TOs). I have reviewed the TSC's TOs and, as I considered appropriate, taken them forward under Assessment Findings (see Annex 1). The TSC TOs provide further guidance to ONR on the GDA Assessment Findings and set initial expectations for ONR to consider when assessing Westinghouse's future submissions regarding their resolution. Within this report, references to the TSC TOs contained in Ref. 17 are provided using the unique TO identifiers (for example, GI-03-TO2.nn).

2.4 Integration with Other Assessment Topics

29. 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.

30. In the assessment, I consulted with the following specialist areas within ONR to clarify the adequacy of Westinghouse's justification proposed against this GDA issue closure (see Ref. 1 for context):

- inspectors working on GI-AP1000-CI-01, GI-AP1000-CI-02, GI-AP1000-CI-04, GI-AP1000-CI-05, GI-AP1000-CI-06, GI-AP1000-CI-07, GI-AP1000-CI-08, GI-AP1000-CI-09 (see also Refs. 60-64), in relation with claims in other C&I safety submissions;
- inspectors working on GI-AP1000-FS-03 and GI-AP1000-FS-04 (see also Ref. 65), in relation with the design change proposal APP-GW-GEE-5251 (Ref. 31); and
- inspectors working on GI-AP1000-EE-01 (see also Ref. 66), in relation with claims in the diversity of the electrical power supply of the C&I systems.

2.5 Out of Scope Items

31. Although to some extent AF-AP1000-CI-036 and AF-AP1000-CI-037 (see Ref. 1) are related to the UK **AP1000** design diversity demonstration, it has already been agreed in GDA Step 4 for these to be resolved post-GDA (Ref. 1) and they were not addressed as part of this GDA issue close-out.

32. The support systems external to the C&I cabinets of the PMS, PLS/DDS and DAS are outside the scope of my assessment of GDA Issue GI-AP1000-CI-03, which focuses on the diversity of the technology of the C&I systems.

3 REQUESTING PARTY'S SAFETY CASE

33. Westinghouse's strategy to address this GDA issue is to include diversity claims in the relevant basis of safety cases (BSCs) and to refer to dedicated documents for their substantiation. The diversity analyses submitted against GI-AP1000-CI-03 are captured in two separate reports:

- Diversity Analysis of the PMS and DAS (UKP-GW-GLR-023, Rev. 0 to 2 in Refs 18, 19 and 45); and
- Diversity Analysis of the PLS DDS and DAS (UKP-GW-GLR-024, Rev. 0 to 2 in Refs 20, 21 and 46).

34. After re-entering GDA, Westinghouse submitted a strategy document (UKP-GW-GL-111, Rev. 0 – Ref. 23) to define the approach it was proposing to the diversity demonstration in anticipation of the main submissions against GI-AP1000-CI-03. It is noted that this document was not originally in the resolution plan for GI-AP1000-CI-03 (Ref. 6). Westinghouse subsequently informed ONR of its intention to withdraw this document, clarifying that UKP-GW-GLR-023 (Rev. 0 to 2 in Refs 18, 19 and 45) and UKP-GW-GLR-024 (Rev. 0 to 2 in Refs 20, 21 and 46) also present the diversity strategy. Therefore, I did not consider Ref. 23 as part of my final judgement on the closure of this GDA issue.

35. In the assessment of UKP-GW-GLR-023 (Rev. 0 to 2 in Refs 18, 19 and 45) and UKP-GW-GLR-024 (Rev. 0 to 2 in Refs 20, 21 and 46), some sections of the following BSCs were reviewed to verify the consistency of the diversity analyses with the safety cases for individual C&I systems:

- DAS BSC (Ref. 24);
- PMS BSC (Ref. 26);
- CIM BSC (Ref. 27);
- blocking device BSC (Ref. 28);
- PLS BSC (Ref. 29); and
- DDS BSC (Ref. 30).

36. Due to the expectation for the design maturity for the DAS within GDA (see Ref. 1 and GI-AP1000-CI-01/GI-AP1000-CI-02 assessment in Ref. 60), in the resolution of GI-AP1000-CI-03 Westinghouse also made reference to the DAS lifecycle document (Ref. 25) as a means of capturing commitments in the design of the secondary protection platform (for example, on human diversity). Where relevant, my assessment has confirmed that the high-level design-seeking decisions in Ref. 25 were in line with the claims made in the submissions against GI-AP1000-CI-03.

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

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

4.1 Scope of Assessment Undertaken

38. The scope of the assessment covered the Westinghouse submissions identified in the GDA Issue resolution plan (Ref. 6). The assessment of these supporting submissions is identified in Refs 16 and 17.

4.2 Assessment

39. The focus of the assessment undertaken in this GDA Issue GI-AP1000-CI-03 close-out is to determine whether the technology, the system interfaces and the design development process proposed by Westinghouse for the UK **AP1000** plant C&I systems provides an adequate level of diversity and demonstrates sufficient evidence to de-risk future phases of the UK **AP1000** detailed design.

40. This assessment covered all of the submissions identified by Westinghouse in the GDA Issue resolution plan (Ref. 6) and the supporting documents as described in Section 3 of this report. It is noted that, although Westinghouse explained that the compliance with SAPs for individual systems was provided in the basis of safety cases for each individual C&I systems (Refs. 60-64), consideration was given in this assessment as to how the submissions against GI-AP1000-CI-03 addressed the key SAPs identified in Section 2.2.1 (see Ref. 17).

4.2.1 Diversity Strategy for the Resolution of GI-AP1000-CI-03 (UKP-GW-GL-111)

41. In the following, the high-level findings that emerged from the assessment of GI-AP1000-CI-03 submissions are presented. A detailed review of the reports is recorded in Ref. 17.

42. The expectation for the closure of this GDA issue is that the diversity analyses provided by Westinghouse are consistent with the claims and the design reference point in the submissions against:

- GI-AP1000-CI-01 and GI-AP1000-CI-02 (on the DAS, Ref. 60);
- GI-AP1000-CI-04 (on the PMS blockers, Ref. 61);
- GI-AP1000-CI-06 and GI-AP1000-CI-07 (on the PLS and DDS, Ref. 62);
- GI-AP1000-CI-08 (on the PMS, Ref. 63); and
- GI-AP1000-CI-09 (on the CIM, Ref. 64).

43. In its early engagement with ONR, Westinghouse highlighted that the finalisation of the diversity analyses for GI-AP1000-CI-03 closure involved the development of the basis of safety cases for the relevant C&I systems. This, in turn, required the completion of other C&I GDA issues as indicated above (see Section 2.4 of this report).

44. To de-risk the schedule for GI-AP1000-CI-03 and to account for other inputs that emerged from the initial discussions with ONR on this GDA issue (see Refs. 39 to 44), Westinghouse submitted a diversity strategy document (UKP-GW-GL-111, Rev. 0 – Ref. 23) containing a high-level description of the approach intended to be used in the formal submissions. I found that Ref. 23 was broadly acceptable, both in terms of diversity standards, such as IEC 62340 (Ref 10) and NUREG 6303 (Ref. 14) and in terms of the approach, based on a CAE trail.

45. While Ref. 23 describes, at high level, the approach to be taken for the diversity analyses, Westinghouse explained that it expected the detailed structure of the CAE to be developed in the formal submissions against GI-AP1000-CI-03. In the assessment of Ref. 23, RQ-AP1000-1494 (Ref. 33) and RQ-AP1000-1597 (Ref. 34) were raised seeking clarity regarding:

- the coverage of the clauses in the relevant standards with the CAE;
- Westinghouse's approach to the resolution of the outstanding GDA Step 4 TOs (see Ref. 1);
- the depth and the scope of the diversity analyses proposed for GI-AP1000-CI-03 resolution; and
- the approach for the identification of potential shared components or paths between C&I systems claimed to be diverse in the BSCs.

46. Westinghouse responded to these RQs in Refs 33 and 34 with a high-level strategy to address these issues in the formal submissions against GI-AP1000-CI-03. In Ref. 34, Westinghouse also clarified its plan not to maintain Ref. 23 and to include the diversity strategy in the diversity analyses (UKP-GW-GLR-023 and UKP-GW-GLR-024, see Section 4.2.2 and 4.2.3 in this report). On this basis, Ref. 23 is not considered further in the context of this GDA issue close-out and the focus of my assessment has been submissions UKP-GW-GLR-023 and UKP-GW-GLR-024 (Rev. 2 in Refs 45 and 46).

4.2.2 Diversity Analysis Between the DAS and the PMS (UKP-GW-GLR-023)

47. Westinghouse submitted the first version of the PMS/DAS diversity analysis (UKP-GW-GLR-023 Rev. 0, Ref. 18). In my assessment of this submission, I considered a number of supporting documents (see Ref. 17 for details), including the current versions of the relevant BSCs (Refs 24 to 30).

48. The purpose of Ref. 18 is to substantiate the diversity claim between the main protection system (PMS) and the secondary protection system (DAS). Refs 22 (Chapter 8 of the PCSR) and 49 claim that the DAS is a diverse line of protection against the frequent faults (namely, events with frequency above 10^{-3} per annum). In this regard, the expectation in the UK is that no single cause of failure shall simultaneously affect the functionality of the primary and the secondary protection system (SAP ESS.18 in Ref. 8).

49. Ref. 18 approaches the diversity demonstration for the DAS and the PMS using a CAE structure. Ref. 18 derives high-level claims from clauses in the key diversity standards, such as IEC 62340 (Ref. 10), NUREG 6303 (Ref. 14) and Seven Party Paper (Ref. 15). These high-level claims are then decomposed into sub-level claims that are substantiated through arguments supported by evidence in the form of references to Westinghouse's **AP1000** documentation (eg design processes, design documentation or BSCs). Ref. 18 presents traceability matrices between clauses in standards and claims in the CAE. At a high level, I found this approach sufficient because it provides confidence on the coverage of the key clauses in relevant standards.

50. Rather than focusing on pairs of PMS and DAS functions and considering them against each frequent fault, Ref. 18 approaches the diversity demonstration from a system-based perspective giving consideration to how any failure in the PMS could affect the functionality of the whole DAS. I found the approach proposed by Westinghouse in Ref. 18 to be conservative and to provide an adequate coverage of the common cause failure (CCF) mechanisms outlined in IEC 62340 (Ref. 10). Where the diversity demonstration needed a refinement, Westinghouse complemented this approach with a function-based approach, eg considering the effect of the failure of a

shared path on the delivery of the PMS/DAS safety functions against a particular fault scenario (see, for example, the following discussions on APP-GW-GEE-5251).

51. As a result of my assessment of Ref. 18, I raised a number of queries in RQ-AP1000-1646 (Ref. 35) and RQ-AP1000-1672 (Ref. 38), mainly regarding:

- need for additional clarity of the design reference point considered in the diversity analysis;
- approach taken by Westinghouse to map clauses in the safety case to standards in the CAE structure and the need to justify the approach as being reasonable;
- need for additional clarity regarding the depth of the diversity analysis (such as confirming that the analysis was carried out at a component rather than a system level); and
- consideration of the CIM and the blockers as part of the PMS in the diversity analysis.

52. I found that Westinghouse's responses to RQ-AP1000-1646 and RQ-AP1000-1672 in Refs 35 and 38 were broadly acceptable and Westinghouse committed to address the issues in detail in the future revisions of this document. In my assessment of Rev. 1 of UKP-GW-GLR-023 (Ref. 19), I found that the claims in the CAE structure from Ref. 19 addressed the key diversity aspects expected to be addressed within GDA, such as in relation to the diversity of technology, tools and design processes and the independence of the C&I systems (with no shared components). The expectation is that a detailed clause-by-clause statement of compliance of the **AP1000** design against IEC 62340 shall be produced by the Licensee as part of the resolution of AF-AP1000-CI-006 post-GDA (see Ref. 1 for context).

53. With regard to claims made on the human diversity between the PMS and the DAS, I sought confirmation that the DAS submissions against GI-AP1000-CI-01 and GI-AP1000-CI-02 (see Ref. 1 and Ref. 60) included a requirement for independence of the teams developing the DAS and the PMS. I was content with the commitment in the DAS lifecycle document (Ref. 25) provided by Westinghouse.

54. In Ref. 19, Westinghouse carried out a screening of the PMS/DAS components which could be prone to CCFs because of the use of similar equipment type or technology. In my assessment of the output of this exercise, I considered that Westinghouse had included the PMS blockers (based on discrete electronics as is the DAS) in the analysis in Ref. 19. Considering the regulatory expectations set for other GDAs (see, for example, Ref. 3), I found Westinghouse's approach in Ref. 19 acceptable, because for simple components such as resistors and transistors it explained how the risk is managed (eg using different suppliers) and for complex components the approach provided the rationale as to how a high-level screening is possible (eg based on the use of analogue versus digital components). Through this exercise, Westinghouse identified a shortlist of components for which a more detailed diversity analysis is required because of the use of similar equipment type or technology (such as analogue amplifiers or software-based uninterruptible power supplies or UPSs). Westinghouse's justification was that the use of different part numbers ensured an adequate level of diversity between these components for the PMS and the DAS. I raised RQ-AP1000-1762 (Ref. 38) to seek clarity as to how resilience to common mode failures could be inferred from different part numbers.

55. In the RQ response to my question (Ref. 38) and in Rev. 2 of UKP-GW-GLR-023 (Ref. 45), Westinghouse clarified that it took consideration of diversity when selecting components for the two C&I systems (eg using different manufacturers for the PMS and the DAS components of similar type or technology). At a high level, I judged

Westinghouse's considerations in Refs 38 and 45 to be broadly adequate. However, depending on the complexity of the component, a more detailed analysis of the failure modes may be required during detailed design when finalising the selection of components for the C&I systems for the UK **AP1000** design, to confirm their independence and diversity. As an example, Westinghouse explained in Ref. 38 that post-GDA it will give consideration to the use of smart devices in the power supplies for the PMS (through the Class 1 Uninterruptible Power Supply System or IDS) and the DAS (with its internal UPSs). The selection of smart devices for the PMS and/or the DAS would need justification from a diversity perspective to ensure that their use does not introduce new CCFs between the two C&I systems (eg justifying how introducing software in the DAS does not impair its diversity from the PMS). As the UK **AP1000** detailed design is expected to be finalised only post-GDA, I raised an Assessment Finding for the licensee to systematically verify that there are no credible common modes for components of similar type or technology used in the PMS and the DAS (see Annex 1, in particular bullet (b)).

56. In sampling the evidence associated with Ref. 18, I focused my attention on the design change proposal APP-GW-GEE-5251 (Ref. 31). Westinghouse proposed this design change as part of the resolution of GDA Issue GI-AP1000-FS-03 and GI-AP1000-FS-04. The design change (Ref. 31) adds a new function to the DAS for the UK **AP1000** plant, namely to actuate the Core Makeup Tanks (CMTs) and isolate the Chemical and Volume Control System dilution sources in boron dilution scenarios in shutdown states. According to Ref. 31, the new functionality in the DAS utilised the PMS intermediate range flux detectors. Ref. 32 provided the As Low As Reasonably Practicable (ALARP) justification from a fault studies perspective, which was assessed by ONR's fault studies inspector as part of the close-out of GI-AP1000-FS-03 and GI-AP1000-FS-04 and is therefore out of scope for GI-AP1000-CI-03 close-out.

57. I considered the design change proposal in Ref. 31 particularly relevant for the purpose of GI-AP1000-CI-03 because it cross connects the neutron flux intermediate range detectors (part of the PMS system in accordance with Ref. 26) to the DAS. This has the potential to affect the claim of diversity between the two C&I systems (eg clauses 7.1.2, 7.1.3 and 7.1.4 in IEC 62340 (Ref. 10) and SAP EDR.2 (Ref. 8). I raised RQ-AP1000-1647 (Ref. 36) to seek clarity regarding the potential for this design change to compromise the independence of the PMS and the DAS. Ref. 37 also requested clarification as to how failures in the PMS do not affect the new functionality in the DAS added via Ref. 31.

58. In the response to RQ-AP1000-1647 (Ref. 36), Westinghouse provided additional confidence regarding:

- unidirectional optic communication between the PMS and the DAS, minimising the risk of propagation of failures from the lower to the higher safety class system and providing electrical isolation between the systems;
- power supply for the intermediate range detector, associated with the higher safety class (Class 1 PMS power supply); and
- diversity between the DAS and the PMS field instrumentation for the protection against the boron dilution scenario in shutdown state (ie the source range neutron detectors for the PMS and intermediate range detectors for the DAS).

59. I found the responses in Ref. 36 broadly acceptable as Westinghouse demonstrated that the new functionality in the DAS does not compromise the overall independence of the two C&I systems (ie the risk is only limited to the new functionality in the DAS). After assessment of Ref. 26, I was content that the source range and the intermediate range detectors are based on different technologies (BF_3 neutron detectors as opposed to fission chamber detectors) and use different amplifiers. However, I

highlighted the need for additional clarification to further de-risk the potential for failure in the PMS affecting the new DAS function introduced with Ref. 31, eg regarding:

- potential for failure of shared components between the two C&I systems (see clause 7.1.3 in IEC 62340 (Ref. 10));
- potential for failure of shared support systems such as power supplies affecting simultaneously both C&I systems (see clause 7.1.3 in IEC 62340 (Ref. 10)); and
- potential for common failure mechanisms which could affect both systems (see clause 7.1.2 in IEC 62340 (Ref. 10)).

60. Westinghouse addressed these concerns in the following revisions of the PMS/DAS diversity analysis (UKP-GW-GLR-023 Rev. 1 and 2 (Refs 19 and 45)), whereby:

- Westinghouse identified the key aspects to be considered during the detailed design of this change proposal in Ref. 31, to minimise the potential for shared components in the path associated with the new DAS functionality.
- Westinghouse provided high-level optioneering as to how the power supply arrangements could be improved to minimise the risk for CCF.
- Westinghouse identified options to address the potential for a PMS software failure identified as a response to RQ-AP1000-1647 (Ref. 36), which could affect the new DAS function in Ref. 31 proposing modifications to the PMS automatic test arrangements for the intermediate range detector PMS cabinet.

61. I judged the information provided in Ref. 45 sufficient to adequately de-risk future phases of the development of this design change. I raised an Assessment Finding to clarify the need for justification of the final detailed design of the change in APP-GW-GEE-5251 and ensure that it reduces the risks ALARP (see Annex 1, in particular bullet (a)).

62. In the close-out of this GDA issue, I considered Westinghouse's response in RQ-AP1000-1683 (Ref. 48) regarding the supporting systems of the C&I platforms. Refs 22 (Chapter 8 of the PCSR) and 48 claim that the PMS and the DAS supporting systems, such as heating, ventilation and air conditioning (HVAC) and essential water, do not introduce common mode failures between the two C&I systems. More precisely, Westinghouse clarified in Ref. 48 that, in a loss of HVAC scenario, the temperature in the standard **AP1000** PMS cabinet room remains acceptable without any need of cooling for more than 72 hours. As for the DAS, Westinghouse clarified in Ref. 48 that the HVAC calculations and recovery strategy after a prolonged loss of HVAC depend on whether the licensee decides to use the DAS cabinet room as a secondary alarm room. Since the detailed justification of the diversity claim between the PMS/DAS supporting systems is not in the scope of this GDA issue and it may require site-specific considerations, such as external temperatures, detailed thermal load, UK-specific technical specifications and operating rules, I judged that it was proportionate to raise an Assessment Finding for the licensee to extend the diversity analysis to the PMS and DAS supporting systems (see Annex 1, in particular bullet (c)). In the resolution of this Assessment Finding, the licensee shall provide additional evidence to support whether any HVAC and/or essential water is needed for the PMS/DAS normal operation and, if so, include their C&I as part of the PMS/DAS diversity demonstration.

63. In conclusion, I found that the DAS/PMS diversity analysis provided in Ref. 45 met the expectation for this GDA issue closure. Section 4.2.4 of this report captures the expectations for this diversity analysis post-GDA, when the detailed design information for the UK **AP1000** design becomes available.

4.2.3 Diversity Analysis Between the DAS and the PLS/DDS (UKP-GW-GLR-024)

64. Westinghouse submitted the first version of the DAS and the PLS/DDS diversity analysis (UKP-GW-GLR-024 Rev. 0, Ref. 20). The assessment of this submission considered a number of supporting documents, including the current versions of the relevant BSCs (Refs 24 to 30).

65. While the PMS/DAS diversity analysis aims at demonstrating their CCF resilience against frequent fault scenarios, the diversity requirement for the DAS and PLS/DDS stems from the need to minimise the risk for CCFs which could result in a spurious operation of the PLS/DDS (ie frequent fault due to their safety classification, Class 2 and 3 respectively) and a coincident loss of the secondary protection system (DAS).

66. In the assessment of Ref. 20, I raised RQ-AP1000-1650 (Ref. 37) and RQ-AP1000-1672 (Ref. 38), identifying similar concerns as found in the assessment of Rev. 0 of the DAS/PMS diversity analysis (Ref. 18, see Section 4.2.2 of this report). In Ref. 38, I also requested a justification as to why some of the aspects addressed in the PMS/DAS diversity analysis in Ref. 45 were not covered in the diversity analysis for the DAS and the PLS/DDS in Ref. 20, including human diversity, signal isolation or cable segregation.

67. Westinghouse submitted UKP-GW-GLR-024 Rev. 1 (Ref. 21), which I found to address the main concerns raised in previous RQs and to provide additional clarity regarding the substantiation of the claims in the CAE structure.

68. In the response to RQ-AP1000-1672 (Ref. 38), Westinghouse clarified its intention to revisit the concern regarding the human diversity between the DAS and the PLS/DDS. During the assessment of Ref. 21, I sought confirmation that a requirement for diversity of teams developing the DAS and the PLS/DDS be added in the latest revision of the DAS lifecycle document (Ref. 25).

69. Refs 45 and 46 also clarified the arrangements for the delivery of the turbine trip function via the DAS and the PMS. Westinghouse explained that signals from both the DAS and the PMS systems are combined in the turbine protection cabinets, which are located within PLS cabinets. While the isolation of the PMS and the turbine protection (in PLS) is required in the standard plant PMS design (Ref. 26), the same requirement is not captured for the DAS in the standard plant design as the DAS is non-safety system according to the US safety classification (see USNRC Standard Review Plan (NUREG-0800), Branch Technical Position 7-19). In the response to RQ-AP1000-1672 (Ref. 38) and RQ-AP1000-1738 (Ref. 51), Westinghouse revised the safety plan for the DAS BSC (Ref. 24), committing to include the new DAS isolation requirements in the DAS/PLS interface specification. I was content that this approach adequately captured the concern and provided a traceable way to track its implementation.

70. Following additional discussions with ONR (see Ref. 55), Westinghouse issued UKP-GW-GLR-024 Rev. 2 (Ref. 46) confirming that for the standard **AP1000** plant there is no requirement for the segregation of the PLS/DDS and the DAS cables because of the safety classification of these C&I systems (classified as non-safety according to US classification, see USNRC Standard Review Plan (NUREG-0800), Branch Technical Position 7-19). Westinghouse also clarified in Ref. 46 that separation between Category A DAS functions and the lower category functions in the PLS/DDS prevents a fault in the plant wiring from cascading into the DAS. I found Westinghouse's justification insufficiently detailed; eg regarding whether there was a potential for an event, such as a fire or other internal hazard, to affect PLS/DAS cables routed in the same cable run and hence result in a spurious actuation of the PLS and the loss of the DAS. Since this issue does not affect the design of the C&I systems and the detailed cable routing for the UK **AP1000** design is only expected post-GDA, I have raised an Assessment Finding for the licensee to provide a justification as to whether cable

segregation between the DAS and PLS/DDS is required for the UK **AP1000** plant (see Annex 1, in particular bullet (d)).

71. For the diversity between the PMS and the DAS (see Section 4.2.2 of this report), I raised an Assessment Finding for evidence to be provided post-GDA that there is diversity of components of similar type or technology when the detailed design of the DAS and the PLS/DDS is completed (see Annex 1, in particular bullet (b)). On the basis of similar considerations provided in Section 4.2.2 of this report for the PMS/DAS, I also raised an Assessment Finding to complete this diversity analysis considering the supporting systems for the PLS/DDS and the DAS (see Annex 1, in particular bullet (d)).

72. In conclusion, I found that the diversity analysis between the DAS and the PLS/DDS provided in Ref. 46 meets my expectations for GDA issue closure. Section 4.2.4 of this report discusses the expectations for this diversity analysis post-GDA, when the detailed design information for the UK **AP1000** design becomes available.

4.2.4 Completion of the Compensating Activities Identified as part of GI-AP1000-CI-03 Close-out

73. In Rev. 2 of UKP-GW-GLR-023 (Ref. 45) and Rev. 2 of UKP-GW-GLR-024 (Ref. 46), Westinghouse highlighted that the compensating measures (CMs) identified as part of the diversity analyses will be addressed when developing the detailed design for the DAS. It is noted that, according to the nomenclature proposed by Westinghouse in Refs 45 and 46, CMs are additional activities which are expected to be completed post-GDA during the development of the UK **AP1000** detailed design. The commitment to complete the outstanding compensating measures is identified in Westinghouse documentation through the safety plan section of the DAS BSC (Ref. 24), requiring an update to UKP-GW-GLR-023 (Ref. 45) and UKP-GW-GLR-024 (Ref. 46). I judged this approach proportionate, considering the expectation for the maturity of the DAS design in GDA (see Ref. 1). I also found this approach acceptable for GDA because the key compensating measures are identified and captured in this GDA issue closure, hence de-risking the future phase of **AP1000** design development. I raised an Assessment Finding for the licensee to complete the diversity analysis to account for the detailed design information available post-GDA, also updating the CAE trail to reflect the availability of UK-specific evidence, where needed (see Annex 1, in particular bullet (f)).

74. In RQ-AP1000-1672 (Ref. 38), Westinghouse also highlighted that a diversity requirement will be specified in the requirement capture for the C&I systems of the UK **AP1000** plant, by including the relevant standards relating to diversity in the general C&I system requirement specification. Ref. 47 provides a description of the Westinghouse requirement capture process and Westinghouse expect to complete this process for the UK **AP1000** design post-GDA. I judged this approach acceptable, because the requirement capture should also account for site-specific issues and licensee's inputs. I raised an Assessment Finding (see Annex 1, in particular bullet (e)) to ensure that the requirement capture for the UK **AP1000** design takes adequate consideration of the diversity requirements between the C&I systems and that the key diversity standards (such as IEC 62340 and NUREG 6303) are included among the top tier codes and standards as per Ref. 47.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

75. My assessment of the latest revision of the submissions against GI-AP1000-CI-03 has identified that, in general, Westinghouse's approach for the diversity demonstration was in line with the expectation in the UK.

76. My judgement is based on:

- Westinghouse's use of the relevant nuclear standards in the UK (such as IEC 62340 and NUREG 6303);
- Westinghouse's consideration of the key ONR SAPs (Table 1);
- Westinghouse's consideration of the expectations in the UK for the extent of evidence required to demonstrate the diversity of the C&I systems to component level; and
- Westinghouse's adoption of a conservative strategy for the diversity demonstration, considering a system-based approach (ie effect of any common mode failures between the two C&I systems) rather than a functional-based approach (ie the potential for CCFs affecting the delivery of the protection against the same initiating event through both C&I systems).

77. In assessing Westinghouse's submissions and coming to this judgement, I verified the consistency of the regulatory approach against other GDAs, such as UK EPR (see Ref. 3).

4.4 Assessment Findings

78. During my assessment I have raised an Assessment Finding for a future licensee to take forward in their site-specific safety submissions. The matters in the Assessment Finding do not undermine the generic safety submission and are primarily concerned with the provision of site-specific safety case evidence. It is anticipated that this site-specific evidence will become available as the project progresses through the detailed design, construction and commissioning stages. The Assessment Finding is presented in Annex 1.

5 CONCLUSIONS

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

80. In conclusion, I am satisfied that Westinghouse's submissions addressed this GDA issue as:

- the relevant SAPs given in Table 1 have been satisfied;
- an adequate application of the key diversity standards (such as IEC 62340 and NUREG 6303) was demonstrated.
- adequate confidence was provided that the technology used for the DAS is diverse from the primary protection system and the control system in the UK **AP1000**.
- commitment was given to utilise, in the detailed design for the UK DAS, a team that is diverse from those developing the PMS, the PLS and the DDS.
- sufficient confidence was provided that the design change proposal in APP-GW-GEE-5251 does not compromise the diversity of the DAS and the PMS.
- compensating activities to be addressed once the detailed design for the UK **AP1000** C&I systems is completed were identified and committed to update these diversity analyses.

81. In the close-out of this GDA issue, I raised an Assessment Finding to capture a number of technical issues that are expected to be addressed post-GDA, when the detailed design information becomes available.

82. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-03 can be closed.

.

6 REFERENCES

1. ONR-GDA-AR-11-006, Rev. 0, Step 4 Control and Instrumentation Assessment of the Westinghouse **AP1000**® Reactor, November 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf
2. ONR-GDA-AP-14-001, Rev. 0, **AP1000** GDA C&I Assessment Plan, April 2015, TRIM 2015/149263.
3. ONR-GDA-AR-11-022, Rev. 1, GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, March 2013. www.onr.org.uk/new-reactors/reports/step-four/close-out/gi-ukepr-ci-01-close-out.pdf
4. ONR Guidance on Mechanics of Assessment, TRIM 2013/204124.
5. GDA Issue Close-out Phase – Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor Control and Instrumentation GDA Issues Closure Guidance Document, February 2015, TRIM 2015/84414.
6. Westinghouse UK **AP1000**® Generic Design Assessment Resolution Plan for GI-AP1000-C&I-03 Diversity of PLS, PMS (including CIM) and DAS, Rev. 4. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-final-res-plans/resolution-plan-gi-ap1000-ci-03.pdf
7. NS-PER-GD-014, Purpose and Scope of Permissioning. www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf
8. Safety Assessment Principles for Nuclear Facilities, ONR, November 2014. www.onr.org.uk/saps/saps2014.pdf
9. NS-TAST-GD-046, Rev. 3, Computer Based Safety Systems, April 2013. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf
10. IEC 62340:2010, Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF).
11. IEC 60709:2004, Nuclear power plants – Instrumentation and control systems important to safety – Separation.
12. IEC 61513:2011, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.
13. IEC 61226:2009, Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions.
14. NUREG/CR 6303, Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, December 1994.
15. Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations. Revision 2010.
16. S.P1641.27.6 – ONR/T2723, Issue 1, Support for **AP1000** C&I GDA Issues resolution – Work Package Description for GI03 Diversity of PLS, PMS (including CIM) and DAS, December 2015, TRIM 2017/30226.
17. S.P1641.40.TSC267.2 – ONR/T2723, Issue 2, Support for **AP1000** C&I GDA Issues Resolution – GI03 Diversity of PLS, PMS (including CIM) and DAS, March 2017, TRIM 2017/80874.
18. UKP-GW-GLR-023, Rev. 0, United Kingdom **AP1000** Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS), June 2016, TRIM 2016/255845.

19. UKP-GW-GLR-023, Rev. 1, United Kingdom **AP1000** Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS), 9 November 2016, TRIM 2016/435951.

20. UKP-GW-GLR-024, Rev. 0, United Kingdom **AP1000** Diversity Analysis of the Plant Control System Data Display and Processing System (PLS DDS) and Diverse Actuation System (DAS), July 2016, TRIM 2016/276068.

21. UKP-GW-GLR-024, Rev. 1, United Kingdom **AP1000** Diversity Analysis of the Plant Control System Data Display and Processing System (PLS DDS) and Diverse Actuation System (DAS), November 2016, TRIM 2016/450914.

22. Westinghouse Electric Company LLC, WEC-REG-1552N – Enclosure 1 – UKP-GW-GL-793 – Revision 1 – **AP1000** Pre-Construction Safety Report – 31 January 2017 – TRIM 2017/43700..

23. UKP-GW-GL-111, Rev. 0, Strategy for the Diversity Analysis of the Diverse Actuation System, September 2015, TRIM 2015/438890.

24. UKP-DAS-GLR-001, Rev. 2, UK **AP1000** Basis of Safety Case for the Diverse Actuation System, December 2016, TRIM 2016/484831.

25. UKP-DAS-GEH-001, Rev. 4, United Kingdom **AP1000** Diverse Actuation System Safety Lifecycle, December 2016, TRIM 2016/482530.

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

27. UKP-PMS-GLR-002, Rev. 2, United Kingdom **AP1000** Component Interface Module Safety Case Basis, December 2016, TRIM 2016/466185.

28. UKP-PMS-GLR-003, Rev. 1, United Kingdom **AP1000** PMS Spurious Operation Basis of Safety Case, December 2016, TRIM 2016/492565.

29. UKP-PLS-GLR-001, Rev. 1, UK **AP1000** Plant Control System Basis of Safety Case, December 2016, TRIM 2016/502539.

30. UKP-DDS-GLR-001, Rev. 1, UK **AP1000** Data Display and Processing System (DDS) Basis of Safety Case, December 2016, TRIM 2016/502541.

31. APP-GW-GEE-5251, Rev. 0, Addition of Diverse Protection for Boron Dilution at Shutdown, May 2016, TRIM 2016/404217.

32. UKP-GW-GL-083, Rev. 0, **AP1000** Flux Protection and Diversity for Frequent Faults, June 2016, TRIM 2016/263885.

33. RQ-AP1000-1494, Comments on the Diversity Strategy Document UKP-GW-GL-111 Revision 0, April 2016, Full Response, TRIM 2016/144157.

34. RQ-AP1000-1597, Further Comments on the Diversity Strategy (GI-AP1000-CI-03), July 2016, Full Response, TRIM 2016/265764.

35. RQ-AP1000-1646, Document Request and Reference Clarification, August 2016, Full Response, TRIM 2016/322713.

36. RQ-AP1000-1647, Clarification on DCP APP-GW-GEE-5251 Revision 0 in Relation with GI-AP1000-CI-03 and GI-AP1000-FS-03/04, September 2016, Full Response, TRIM 2016/355079.

37. RQ-AP1000-1650, Document Request (CI-03 UKP-GW-GLR-024 Rev 0), July 2016, Full Response, TRIM 2016/304424.

38. RQ-AP1000-1672, Comments on the Diversity Analyses (GI-AP1000-CI-03 UKP-GW-GLR-023 Rev. 0 and UKP-GW-GLR-024 Rev. 0), Paolo Picca, 29 September 2016, Full Response, TRIM 2016/380907.

39. ONR-GDA-CR-14-289, AP1000 C&I GDA Issues Resolution, Contact record for the C&I level 4 meeting, February 2015, TRIM 2015/62150.

40. ONR-GDA-CR-15-114, AP1000 C&I GDA Issues Resolution, Contact record for the C&I level 4 meeting, June 2015, TRIM 2015/255532.

41. ONR-GDA-CR-15-153, AP1000 C&I GDA Issues Resolution, Contact record for the C&I level 4 meeting, July 2015, TRIM 2015/292435.

42. ONR-GDA-CR-15-241, AP1000 C&I GDA Issues Resolution, Contact record for the C&I level 4 meeting, Sept–Oct 2015, TRIM 2015/387616.

43. ONR-NR-CR-16-517, AP1000 Control and Instrumentation GDA Issues Resolution, Contact record for the C&I level 4 meeting, September 2016, TRIM 2016/366564.

44. ONR-NR-CR-16-712, AP1000 C&I GDA Issues Resolution, Contact record for the C&I level 4 meeting, November 2016, TRIM 2016/446970.

45. UKP-GW-GLR-023, Rev. 2, United Kingdom **AP1000** Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS), December 2016, TRIM 2016/502495.

46. UKP-GW-GLR-024, Rev. 2, United Kingdom **AP1000** Diversity Analysis of the Plant Control System/Data Display and Processing System (PLS/DDS) and Diverse Actuation System (DAS), December 2016, TRIM 2016/502496.

47. UKP-GW-GLR-116, Rev. 0, United Kingdom **AP1000** Design C&I Requirements Management Overview, November 2016, TRIM 2016/449029.

48. RQ-AP1000-1683, HVAC Claims on the Fault Schedule (GI-AP1000-FS-08), October 2016, Full Response, TRIM 2016/388850.

49. UKP-GW-GL-067, Rev. 1, **AP1000** Assessment of Diverse Mitigation of Frequent Faults for the UK, TRIM 2015/309272.

50. ONR Assessment Rating Guide, Rev. 0, April 2016, TRIM 2016/118638.

51. RQ-AP1000-1738, DAS SAP Compliance Review, November 2016, Full Response, TRIM 2016/450553.

52. ONR-GDA-GD-001, Rev. 3, New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties. www.onr.org.uk/new-reactors/ngn03.pdf

53. NS-TAST-GD-051, Rev. 4, The purpose, scope and content of safety cases. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

54. Westinghouse UK **AP1000**® Generic Design Assessment Resolution Plan for GI-AP1000-CC-02 PCSR, Rev. 3. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf

55. ONR-NR-CR-16-825, **AP1000** C&I GDA Issues Resolution, Progress C&I level 4 meeting, December 2016, TRIM 2016/499847.

56. UK **AP1000** GDA Step 4 report and publications, ONR website: www.onr.org.uk/new-reactors/ap1000/reports.htm

57. Generic Design Assessment (GDA) of new nuclear power stations, ONR website: www.onr.org.uk/new-reactors/index.htm

58. NS-TAST-GD-003, Rev. 7, Safety Systems, April 2013. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.pdf

59. IEC 61508:2010, Nuclear power plants – Functional safety of electrical/ electronic/programmable electronic safety-related systems.

60. ONR-NR-AR-16-029 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-01 and GI-AP1000-CI-02, TRIM 2016/274937.

61. ONR-NR-AR-16-031 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-04, TRIM 2016/274942.

62. ONR-NR-AR-16-033 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-06 and GI-AP1000-CI-07, TRIM 2016/274944.

63. ONR-NR-AR-16-034 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-08, TRIM 2016/274946.

64. ONR-NR-AR-16-035 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-09, TRIM 2016/274947.

65. ONR-NR-AR-16-033 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-FS-03 and GI-AP1000-FS-04, TRIM 2016/274914.

66. ONR-NR-AR-16-043 - AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-EE-01, TRIM 2016/274980.

Annex 1

Assessment Findings to be addressed during the Forward Programme – GI-AP1000-CI-03

Assessment Finding Number	Assessment Finding	Report Section Reference
CP-AF-AP1000-CI-005	The Licensee shall complete and update the PMS versus DAS and PLS/DDS versus DAS diversity analyses, considering the detailed design for the C&I systems to be used in the UK **AP1000** design. This should include but is not limited to: a) ensure that the implementation of the design change proposal APP-GW-GEE-5251 provides adequate level of diversity and implements the compensating activities identified in UKP-GW-GLR-023, Rev. 2. b) justify the use of diversity in the detailed design and/or selection of components of similar technology or type in the DAS, PMS and PLS/DDS. c) extend the diversity analyses to the supporting systems needed for the DAS, PMS, PLS and DDS systems. d) justify the cable segregation requirements specified for the installation of the DAS and PLS/DDS cables. e) ensure that the requirement specification process for the UK **AP1000** design incorporates IEC 62340 in the top tier of the codes and standards. For further guidance on this Assessment Finding, see Section 4.2 of this report and Technical Observations GI-03-T02-2.1.2.4.2.1-1, GI-03-T02-2.1.2.4.2.1-2, GI-03-TO2-2.1.2.4.2.3-1, GI-03-T02-2.1.2.4.2.3-2, GI-03-T02-2.1.2.4.2.3-5, GI-03-T02-2.1.2.4.2.3-6, GI-03-T02-2.1.2.4.2.3-7, GI-03-T02-2.1.2.4.2.3-8, GI-03-T02-2.1.2.4.2.3-9, GI-03-T02-2.1.2.4.2.3-11, GI-03-TO2-2.1.2.4.2.5-1, GI-03-TO2-2.1.2.4.2.5-2, GI-03-TO2-2.1.2.4.2.5-3, GI-03-T02-2.1.2.5.2.1-2, GI-03-T02-2.1.2.5.2.1-3, GI-03-T02-2.1.2.5.2.3-1, GI-03-T02-2.1.2.6.2.3-1 and GI-03-T02-2.1.2.7.2-1 in Ref. 17.	Sections 4.2.1, 4.2.2 and 4.2.3