New Reactors Programme

GDA close-out for the AP1000® Pressurised Water Reactor

GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0 DAS – Adequacy of Architecture

Assessment Report: ONR-NR-AR-16-029
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

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

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP-1000-CI-02 Revision 0 DAS – Adequacy of Architecture.

These GDA issues arose in Step 4 due to the need to:

- improve the quality of the diverse actuation system (DAS) safety justification;
- ensure that the DAS would remain in service during reactor operation including during maintenance activities; and
- incorporate formally the Westinghouse 7300 series based DAS into the UK **AP1000** reactor C&I design.

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

- provide a basis of safety case (BSC) for the DAS that met ONR expectations;
- submit key documents in support of the BSC;
- make available further documents that support the BSC as requested by ONR; and
- provide the design change proposals (DCPs) for the Westinghouse 7300 series DAS.

My assessment conclusion is that the:

- safety case for the DAS has been significantly improved through the provision of the BSC and its references, and is adequate for the conceptual design presented during GDA;
- additional redundancy provided by the modified architecture allows maintenance to be undertaken during power operation without the need to remove the DAS from service;
- DAS DCPs have formally introduced the 7300 series DAS into the UK **AP1000** reactor C&I design and the DCPs address the ONR concerns raised at Step 4.

My judgement is based on the following factors:

- review of the main safety submissions such as the DAS BSC as identified in the resolution plan and sampling of key supporting documents;
- Westinghouse's improvements to the number of redundant sensor channels and the voting logic provided for these channels within the DAS architecture;
- Westinghouse's commitment to modify the voting logic provided the safety and transient analyses to be undertaken post-GDA demonstrate that the proposed change is acceptable;
- adoption by Westinghouse of modern standards for the design of the DAS and satisfaction of key Safety Assessment Principles (SAPs); and
- review of the DAS DCPs and their inclusion in the design reference point.

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 DAS BSC as the detailed design and implementation of the DAS is completed post-GDA;
- complete the SAP claims, arguments and evidence (CAE) and standards conformance demonstrations by including design and implementation detail such as verification, validation and commissioning test records; and
- document and justify the reliability of the final detailed DAS design in the safety case.

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

In summary, I am satisfied that GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP-1000-CI-02 Revision 0 DAS – Adequacy of Architecture can be closed.

LIST OF ABBREVIATIONS

1oo2	one-out-of-two
(1oo2)x2	one-out-of-two taken twice
2oo2	two-out-of-two
2oo3	two-out-of-three
2oo4	two-out-of-four
ADS	automatic depressurisation system
ALARP	As Low As Reasonably Practicable
ALS	advanced logic system
BSC	basis of safety case
C&I	control and instrumentation
CAE	claims, arguments and evidence
CCF	common cause failure
CIM	component interface module
DAC	Design Acceptance Confirmation
DAS	diverse actuation system
DCP	design change proposal
EMI	Electro-magnetic interference
ESF	engineered safety features
ESFAS	engineered safety features actuation system
EQ	equipment qualification
FPGA	field programmable gate array
GDA	Generic Design Assessment
IEC	International Electrotechnical Commission
IDAC	Interim Design Acceptance Confirmation
IRWST	in-containment refuelling water storage tank
MCR	main control room
MDEP	multi-national design evaluation programme
ONR	Office for Nuclear Regulation
PCSR	Pre-construction Safety Report
pfd	probability of failure on demand
PLS	Plant control system
PMS	Protection and safety monitoring system
PSA	probabilistic safety assessment
PSR	Preliminary Safety Report
RFI	radio frequency interference
RQ	Regulatory Query
SAPs	Safety Assessment Principles

SIL	safety integrity level
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor
UPS	uninterruptible power supplies

TABLE OF CONTENTS

Tables

Annex

1 INTRODUCTION

1.1 Background

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

2. This report is the ONR's assessment of the Westinghouse AP1000® pressurised water reactor design in the area of C&I. Specifically this report addresses GDA issues GI-AP1000-CI-01 Revision 0, DAS – Adequacy of Safety Case and GI-AP-1000-CI-02 Revision 0 DAS – Adequacy of Architecture.

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

1.2 Scope

4. The scope of this assessment is detailed in AP1000 GDA C&I Assessment Plan ONR-GDA-AP-14-001 Rev 0, (Ref. 38).

5. The scope of assessment focused on:

- the formal introduction of the DAS DCPs (action GI-AP1000-C&I-01.A1);
- the BSC for the DAS (Ref. 3), which is the key submission addressing the GDA issues (action: GI-AP1000-C&I-01.A2);
- sampling of key references to the BSC, including those identified in the Westinghouse resolution plan (Ref. 2);
- proposed DAS architecture so as to ensure that the DAS would remain in service during reactor operation, including during maintenance activities (action: GI-AP1000-C&I-02.A1); and
- substantiation that the automatic and manual DAS meet their reliability targets (action; GI-AP1000-C&I-02.A2).

6. My assessment addressed the key areas of concern identified during GDA Step 4: the need to improve the quality of the DAS safety case through the submission of a BSC and supporting references; and to ensure that the DAS would remain in service during reactor operation. The GDA submission should be consistent with that of a Pre-construction Safety Report (PCSR) but the C&I Step 4 submissions fell short of this expectation. In addition, the DAS design changes needed to be formally recorded by raising Westinghouse's DCPs prior to GDA closure.

7. GDA issue action GI-AP1000-C&I-02.A3 required Westinghouse to identify and provide a description of the sources of electric power for the DAS and their physical location on the plant. The ONR electrical team undertook the assessment of this GDA issue action. They found that the submission satisfactorily addressed the GDA issue action (See ONR assessment report GDA Issue GI-AP1000-EE-01 – PCSR Presentation of Claims, Arguments and Evidence, Ref. 34).

8. The scope of assessment is appropriate for GDA because it ensured that an adequate safety justification had been set out prior to the detailed design and implementation of the DAS, 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 in a PCSR and supporting references such as the DAS BSC (see ONR, New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties – www.onr.org.uk/new-reactors/guidance-assessment.htm). In addition, the assessment focused on the key areas 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 DAS BSC and key references identified in the Westinghouse resolution plan and DAS BSC. To follow the evidence trail, I also included sampling of selected references identified during the reviews of the DAS BSC and the key references.

2 ASSESSMENT STRATEGY

2.1 Pre-construction Safety Report (PCSR)

11. ONR's New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties (www.onr.org.uk/new-reactors/guidance-assessment.htm) 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/index.htm)

12. At the end of Step 4, ONR and the Environment Agency raised GDA issue CC-02 (www.onr.org.uk/new-reactors/ap1000/gda-issues-res-plan.htm) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the CAE to substantiate the adequacy of the **AP1000** reactor design reference point.

13. A separate regulatory assessment report considers the adequacy of the PCSR and closure of GDA issue CC-02. Therefore, this report does not discuss the C&I aspects of the PCSR. This assessment focuses on the supporting documents and evidence specific to GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP-1000-CI-02 Revision 0 DAS – Adequacy of Architecture.

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment are principally the SAPs (Ref. 17), internal TAGs (Ref. 18), relevant national and international standards and relevant good practice informed by existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles (SAPs)

15. The key SAPs applied in the assessment are included in Table 1. Note that the full scope of SAPs applicable to C&I assessment and considered during GDA Step 4 can be found in Ref. 19 (Table 4).

Table 1 – Key Safety Assessment Principles

ESS	All ESS SAPS, since the DAS is a safety system (responds to plant events to shut reactor down) and is Class 2 in alignment with International Electrotechnical Commission (IEC) 61226 (clause 7.3.2.1). The following ESS SAPs are of particular relevance given the topics covered by the GDA issues.
ESS.2	Determination of SS requirements
ESS.8	Automatic initiation
ESS.9	Time for human intervention
ESS.11	Demonstration of adequacy – fault schedule, led to the determination of the DAS functions, response time, trip settings and reliability targets.
ESS.18	Failure independence. Given the specific arrangement of the DAS cabinets and need for independence and segregation.
ESS.21	Reliability. Confirm fail safe approach and means of detecting internal faults.
ESS.23	Unavailability of equipment
ECS.1 and 2	Categorisation and classification

EKP.5	Safety measures
EDR.1 to 4	Failure to safety; redundancy, diversity and segregation; common cause failure; single failure criterion.
ERL.1 to 3	Reliability claims
EMT.7	Maintenance, inspection and testing – should not lead to loss of safety function. Important part of the DAS architecture justification.

2.2.2 Technical Assessment Guides

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

Table 2 – Technical Assessment Guides

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

2.2.3 National and International Standards and Guidance

17. The international standards and guidance that have been used 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 60980:1989	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations
IEC 61000: (series)	Electromagnetic compatibility

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 DAS BSC (Ref. 3), SAP CAEs (Ref. 4) and IEC 61508-2 Compliance (Ref. 5) plus sampling of selected references identified during the reviews of Refs. 3, 4 and 5.
"	Review of DAS Design Process Document UKP-DAS-GEH-001 Rev 1, Ref. 6 and DAS Safety Lifecycle UKP-DAS-GEH-001 Rev. 2, Ref. 16.
"	Review of DAS Qualification Assessment, as provided in Westinghouse letter WEC-REG-0328N, Ref. 7.
"	Review of DAS Failure mode, effects and criticality analysis (FMECA) documentation UKP-DAS-GLR-004, Ref. 8 and DAS Reliability Analysis Report UKP-DAS-GLR-003, Ref. 9.
"	Review of DAS Architecture Drawings UKP-DAS-J0-001 (sheets 001 to 043), Ref. 10 and Functional Logic Diagrams UKP-DAS-J3-001 (sheets 001 to 026), Ref. 11.
"	DAS DCP reviews – Changes to Diverse Actuation System (DAS) Voting Logic and Associated Architecture APP-GW-GEE-2286, Ref. 12 and Changes to Diverse Actuation System (DAS) Platform Implementation APP-GW-GEE-2287, Ref. 13.

20. The TSC undertook the technical reviews under the ONR's close direction and supervision. The regulatory judgement on the adequacy or otherwise of the **AP1000** reactor was made exclusively by ONR. ONR raised all Regulatory Queries (RQs) and meeting actions with Westinghouse. RQs are requests by ONR for clarification and additional information and are not necessarily indicative of any perceived shortfall. The location of all RQs (for example, RQ-AP1000-xxxx, where xxxx is the unique identifier number) in ONR's document management system – TRIM – can be identified through Ref. 23.

21. The TSC provided a report (Ref. 20) that addresses the scope of work listed above. The TSC also reviewed responses to RQs and meeting actions placed on Westinghouse. The TSC report (Ref. 20) includes a summary statement of the results of its work and findings – Technical Observations (TOs). I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under assessment findings (see below and Annex 1). The TSC TOs provide further guidance on the GDA assessment findings and their means of resolution. In my report references to the TSC TOs contained in Ref. 20 are provided using the unique TO identifiers (for example, CI-xx.TO1/2-mmmm.nn, where mmmm is the Ref. 20 report section containing the TO description and nn is the unique TO identifier within that section).

2.4 Integration With Other Assessment Topics

22. GDA requires the submission of an adequate, coherent and holistic generic safety case. Therefore, regulatory assessment cannot be carried out in isolation as there are

often safety issues of a multi-topic or cross-cutting nature. The ONR electrical team undertook the assessment of action GI-AP1000-C&I-02.A3 (Ref. 34). I consulted the ONR probabilistic safety assessment (PSA) team (Ref 26) in relation to modelling of DAS reliability in the PSA. The ONR internal hazards team considered internal hazards, such as fire, that could adversely affect the DAS. The ONR fault studies team were consulted about the relative merits of (1oo2)x2 versus 2oo4 voting logic architecture, in particular in relation to asymmetric reactor faults (Ref. 36).

2.5 Out-of-scope Items

23. The items that are outside the scope of GDA are identified in the Step 4 C&I assessment report (Ref. 19). The availability of evidence is identified in Ref. 19 as follows:

- A – all evidence for that phase 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 DAS platform (that is, the Westinghouse 7300 series equipment) it was noted that the Platform Description documentation is defined as category A and Platform Qualification as B*, where B* was defined as “B* Original 7300 series qualification documentation will be available but the DAS system will be qualified to the **AP1000** requirements before deployment”.

25. In relation to the implementation of the DAS using the 7300 series platform, the availability of documentation for GDA assessment declared by Westinghouse (see Ref. 19) is as shown in Table 5.

Table 5 – Availability of DAS documentation for GDA assessment

Lifecycle phase	Availability Category
Design requirements	B
System definition	B
Design	B
Implementation	B
Test	B
Installation	B

26. The significance of Westinghouse defining the Availability Category as B is that not all process output records were available for review during GDA (for example, test or

verification records as required by the UK AP1000 reactor DAS safety lifecycle, Ref. 5). However, Westinghouse has defined the design and implementation processes in accordance with appropriate standards (for example, IEC 61508-2). I consider the level of detail is acceptable as it aligns with what is expected for a PCSR and recognises that the UK **AP1000** reactor DAS, using the 7300 series Westinghouse platform, is a new concept with no previous system development and implementation history.

3 REQUESTING PARTY'S SAFETY CASE

27. Westinghouse's safety case for the DAS is based on the presentation of a BSC along with supporting references that demonstrate that the DAS satisfies the GDA issues and is capable of remaining in service during operation. The Westinghouse safety case for GDA issues GI-AP1000-CI-01 Revision 0, DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0, DAS – Adequacy of Architecture is documented in:

- United Kingdom UK AP1000 Basis of Safety Case for the 7300 Series Diverse Actuation System – UKP-DAS-GLR-001, Rev. 1, Ref. 3, which is the main submission addressing the GDA issues;
- key references to the BSC, including those identified in the Westinghouse resolution plan, Ref. 2:
    - United Kingdom UK AP1000 Diverse Actuation System Safety Assessment Principle Compliance – UKP-DAS-GLR-005, Rev. 0, Ref. 4;
    - United Kingdom AP1000 Diverse Actuation System IEC 61508-2 Compliance – UKP-DAS-GLR-002, Rev. 0, Ref. 5;
    - United Kingdom AP1000 Diverse Actuation System Safety Lifecycle – UKP-DAS-GEH-001, Rev. 2, Ref. 16; and
    - DAS Qualification Assessment – Westinghouse letter WEC-REG-0328N, Ref. 7.
- DAS DCPs that provide the formal introduction of the DAS into the UK **AP1000** reactor design:
    - DAS DCP – Changes to Diverse Actuation System (DAS) Voting Logic and Associated Architecture – APP-GW-GEE-2286, Ref. 12;
    - DAS DCP – Changes to Diverse Actuation System (DAS) Platform Implementation – APP-GW-GEE-2287, Ref. 13;
    - DAS DCP – Modifications to Diverse Actuation System – APP-GW-GEE-3001, Ref. 14; and
    - DAS DCP – Corrections to Power Sources for Diverse Actuation System – APP-GW-GEE-4517, Ref. 15.
- DAS architecture drawings – United Kingdom AP1000 Diverse Actuation System Architecture Drawings UKP-DAS-J0-001 (sheets 001 to 043), Ref. 10;
- DAS logic drawings – United Kingdom AP1000 Diverse Actuation System Functional Logic Diagrams UKP-DAS-J3-001 (sheets 001 to 026), Ref. 11;
- submissions that provide substantiation that the automatic and manual DAS meet their reliability targets;
    - DAS FMECA documentation – United Kingdom AP1000 Diverse Actuation System Failure Modes, Effects and Criticality Analysis – UKP-DAS-GLR-004, Ref. 8; and
    - DAS Reliability Analysis Report – United Kingdom AP1000 Diverse Actuation System Reliability Analysis Report – UKP-DAS-GLR-003, Ref. 9.

4 ONR ASSESSMENT OF GDA ISSUES GI-AP1000-CI-01 REVISION 0, DAS – ADEQUACY OF SAFETY CASE AND GI-AP1000-CI-02 REVISION 0, DAS – ADEQUACY OF ARCHITECTURE

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

4.1 Scope of Assessment Undertaken

29. The scope of my assessment covered the Westinghouse submissions identified in the GDA issue resolution plan (Ref. 2). This included the DAS BSC (Ref. 3), DAS DCPs (Refs. 12 to 15), architecture and logic drawings (Refs. 10 and 11), DAS qualification assessment (Ref. 7) and reliability submissions (Refs. 8 and 9). I also reviewed the DAS SAP CAE submission (Ref. 4), DAS Safety Lifecycle Document (Ref. 16) and DAS IEC 61508-2 compliance assessment (Ref. 5). The submissions made by Westinghouse in this area may address GDA Step 4 assessment findings (see Ref. 19). 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 below my assessment of Westinghouse's submissions provided in response to GDA issues GI-AP1000-CI-01 Revision 0, DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0, DAS –Adequacy of Architecture for the DAS. GDA issue GI-AP1000-CI-01 has three associated actions and GI-AP1000-CI-02 has two. I reviewed the submissions provided in response to the actions and raised clarification requests by RQ. As appropriate, Westinghouse revised the submitted documents to address the points raised in the RQs. The description of the scope of work performed by the TSC in support of my assessment, and the TOs arising from their work, are contained in a TSC report (Ref. 20).

31. The DAS provides a diverse means of automatic reactor trip and actuation of the engineered safety features (ESF) as a backup to the PMS. The DAS also has a manual section that duplicates the automatic functions and enables manual actuation of additional ESFs , for example, operation of the automatic depressurisation system (ADS) valves. The DAS has three cabinets in a room in the auxiliary building and a DAS control panel in the main control room (MCR). The **AP1000** reactor PCSR Chapter 8 – Fault and Accident Analysis (Ref. 40) identifies the events for which the DAS provides mitigation.

32. The original 2oo2 field programmable gate array (FPGA) based design was such that the DAS would need to be withdrawn from service for routine maintenance and repair during reactor power operation. The DAS would also be unavailable in the event of a single random hardware failure. In both of the above cases, the **AP1000** reactor would lose its 'secondary' protection system.

33. The revised DAS design submitted by Westinghouse in response to the GDA issue is a non-computerised system arranged to provide either 2oo3 or (1oo2)x2 voting logic for the input signals, as follows:

- temperature of the reactor coolant system hot leg feeding the heat exchanger inlet – (1oo2)x2,
- steam generator level – (1oo2)x2,
- pressuriser level – 2oo3,
- containment temperature – 2oo3.

34. I provide comments below on the use of (1oo2)x2 logic as opposed to 2oo4 voting logic. These changes improve the availability of the DAS and its fault tolerance. The design changes also improve the diversity of the DAS from the Protection and Safety Monitoring System (PMS) Component Interface Module (CIM) by avoiding the use of common FPGA technology and the same company for design and implementation. The PMS is the **AP1000** reactor's primary protection system. The DAS is built from a number of different Westinghouse 7300 series platform conventional electronic modules that are selected and configured to achieve the required safety functions.

4.2.1 GDA Issue Action GI-AP1000-C&I-01.A1 Introduction of DAS Changes via the DCP.

35. In this part of my assessment, I reviewed Westinghouse's response to GDA issue action GI-AP1000-C&I-01.A1. The GDA issue action requires Westinghouse to introduce formally the change to the architecture and technology of the DAS via the design change process. The DAS DCPs that provide the formal introduction of the DAS into the UK **AP1000** reactor design, as noted in the Westinghouse resolution plan, are Refs 12, 13, 14 and 15. Note that references 14 and 15 are standard plant changes that have already been incorporated into the reactor's design.

36. I reviewed the DCPs and found that Ref. 12 formally introduces the changes to the DAS logic and architecture. Assessment of the DAS logic and architecture drawings is contained under GDA issue action GI-AP1000-CI-02.A1in section 4.2.3 below.

37. Ref 13 introduces the change from the advanced logic system (ALS) FPGA-based platform to one based on the Westinghouse 7300 series conventional electronics equipment. The DCP formally introduces this change and addresses a concern raised by ONR in relation to diversity of the DAS and PMS (CIM) given both were based on the same FPGA technology from a single supplier and used the same company for design and implementation.

38. Westinghouse raised Ref. 14 to address a number of identified deficiencies, such as the need to address a concern where all equipment required to generate a squib valve actuation is in one cabinet. This means that a fire in that cabinet could induce a spurious squib valve actuation. ADS Stage 4, In-containment refuelling water storage tank (IRWST) injection, IRWST drain, and containment recirculation are the manual DAS functions that actuate squib valves.

39. Westinghouse is to change the DAS design by adding an additional cabinet to the auxiliary building room that currently houses the DAS cabinets, removing both the DAS cabinets in the annex building and moving their functionality to the cabinets in the auxiliary building room. There will be three cabinets in the auxiliary building: two processor cabinets and one squib valve controller cabinet. The squib valve 'ARM' hardware will be in one processor cabinet, and the 'ACTUATE' hardware in the other. As a result, fire in one processor cabinet will not actuate a squib valve, since both 'ARM' and 'ACTUATE' signals are required. The DCP also addresses other necessary changes for the UK DAS design (note: the DCP includes changes related to the ALS-based DAS provisions that are not relevant to the UK 7300 series DAS).

40. Ref.15 proposes to re-assign DAS cabinet power supplies so that the DAS has diesel generator back-up support from both diesel generators. The power supplies were previously backed-up by both diesel generators but were inadvertently put onto the same diesel generator as a result of another DCP. As such, this is a necessary change to the DAS power supply arrangements, which Westinghouse has included within the UK **AP1000** reactor design.

41. I am content that the Westinghouse 7300 series DAS has been formally introduced into the UK **AP1000** reactor design by the DCPs submitted by Westinghouse (Refs.

12, 13, 14 and 15), and their inclusion in the design reference point (Ref. 39). GDA issue action GI-AP1000-C&I-01.A1 can be closed.

4.2.2 GDA Issue Action GI-AP1000-CI-01.A2 – Westinghouse to provide the BSC for the DAS

42. In this section, I provide my assessment of Westinghouse's response to GDA issue action GI-AP1000-CI-01.A2, which required Westinghouse to provide a BSC for the DAS. The key document provided by Westinghouse in relation to closure of GDA issue action GI-AP1000-CI-01.A2 – Adequacy of DAS Safety Case, is the DAS BSC Ref. 3. The GDA issue, as defined in Ref. 19, outlines the expectations for a BSC. I provided further guidance to Westinghouse on the expectations for a BSC in a document entitled Control and Instrumentation GDA Issues Closure Guidance Document (Ref. 21). However, in the letter supplying this document (Ref. 22), I explained to Westinghouse that it is the requesting party's responsibility to consider and provide a comprehensive safety submission addressing each of the GDA issues.

43. I reviewed Ref. 3 to:

- confirm that the submission adequately addresses the topics and elements of a BSC, as outlined in the GDA issue and ONR GDA issues Closure Guidance Document Ref. 21;
- assess fulfilment of the commitments contained in the Westinghouse resolution plan;
- determine if it addresses TOs relevant to closure of the GDA issue (Ref. 19 contains a description of the TOs); and
- check the adequacy of the CAE trail for the DAS lifecycle (for example, to see if IEC 61513 section 6 'Overall I&C safety life cycle' was adequately addressed).

44. Ref. 3 provides a demonstration of conformance to an IEC 61513 safety lifecycle (section 5) and applicable SAPs (subsection 6.1.3.1, which references Ref. 4). Ref. 3 also explains why Westinghouse considers that the DAS design satisfies As Low As Reasonably Practicable (ALARP) principles (section 7.1) and outlines the production excellence demonstration (subsections 6.1.4 to 6.1.7, 6.10 and 6.2). The safety plan presented in Ref. 3 (section 4) provides a schedule for the production of future DAS safety demonstrations and safety lifecycle activities not completed during GDA. This includes production of evidence required to address gaps in the SAP (Ref. 4) and standard's conformance demonstrations (Ref. 5). Section 8 of Ref. 3 outlines the manner of closure of relevant Step 4 TOs. My review of the supporting submissions, identified below, included consideration of whether Westinghouse had satisfactorily addressed Step 4 TOs.

45. Westinghouse will update the safety case documentation (for example, BSC and compliance assessments, and so on) as the detailed design of the DAS is finalised and implemented post-GDA. For example, to document closure of the gaps identified in the safety plan. The implementation detail for the DAS design presented during GDA (see out of scope section 2.5) is not complete, however, it is sufficient to demonstrate that no significant safety issues remain (that is, that would present a risk of major DAS issues emerging post-GDA). 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 during this phase.

46. Ref. 3 includes safety lifecycle claims (based on IEC 61513) that address topics such as:

- functional and performance requirements,

- defence-in-depth,
- interfaces,
- Equipment Qualification (EQ),
- internal and external hazards,
- operation,
- maintenance.

47. I reviewed Ref. 3 and raised a number of queries with Westinghouse (RQ-AP1000-1719 and RQ-AP1000-1740) for example, asking Westinghouse to:

- clarify the functional and performance requirements, (that is, safety functions to be performed and required response time);
- clarify the hazards affecting DAS cabinets;
- explain the relevance of the 7300 series platform operating experience to the safety case;
- clarify the relevance of a statement in Ref. 3 that notes there is an out-of-service period during power operation;
- clarify the actions taken following loss of DAS power;
- clarify the approach used for the 7300 series platform IEC 61508-2 conformance demonstration; and
- provide a definition of responsibilities between Westinghouse and the licensee (for example, in relation to those described in Ref. 3's safety plan section).

48. In response to the RQs, Westinghouse stated that fire is the only significant hazard that can affect the DAS cabinets, a fire would conservatively affect all cabinets and the PMS would be unaffected (see also discussion above on Ref. 14 in section 4.2.1). Hence, rearrangement of the functions across DAS cabinets would provide minimal benefit. The ONR internal hazards team assessed the potential for internal hazards such as fire to adversely affect the DAS (see ONR Assessment Report ONR-NR-AR-16-020 Internal Hazards GDA issues GI-AP1000-IH-01 to IH-06, Ref. 41) and are broadly satisfied with the arguments presented on the location of the DAS cabinets.

49. Westinghouse confirmed that the operating experience identified in the 7300 Process Protection and Control System Life Cycle Management Planning Sourcebook, Ref. 31 (as cited in the DAS BSC) is relatable to the UK **AP1000** reactor DAS and its 'energise-to-actuate' architecture. The DAS energise-to-actuate architecture requires power to be available in order to fulfil its safety functions. The DAS is provided with dual Uninterruptible Power Supplies (UPSs), which improve power supply availability and provide protection against single random hardware failures. Westinghouse provided a comprehensive response regarding the action taken on detection of a DAS power supply failure (for example, annunciation of alarms in the MCR and dispatch of an operator to the DAS cabinets to investigate the cause of the alarm).

50. Westinghouse clarified that there is no out-of-service period during power operation. Westinghouse provided a commitment to include response time requirements into the System Requirements Documents post-GDA. Westinghouse confirmed a proven-in-use case will be presented for the DAS platform (boards) and clarified the responsibilities for activities described in Ref. 3's safety plan section. Westinghouse revised Ref. 3 (that is, Ref. 28) to incorporate the necessary clarifications.

51. Ref. 3 presents an explanation of the use of IEC 61508-2 for the DAS hardware design since there is no nuclear equivalent standard for hardware-based systems. As the DAS

reliability claim is 10-2 probability of failure on demand (PFD) my expectation is (see NS-TAST-GD-046) that safety integrity level (SIL) 2 requirements would be adopted (for example, in relation to selection of techniques and measures to address random hardware and systematic failures). Section 6.1.8.2 of Ref. 3 satisfies my expectation by stating the appropriate integrity level for the DAS is SIL 2.

52. Westinghouse's approach to demonstrating conformance to the IEC 61513 safety lifecycle is contained in Ref. 3 section 5.1. A tabular CAE trail approach is used that only includes 'shall' clauses and certain objectives clauses (that is, as confirmed in the response to RQ-AP1000-1594). The IEC 61513 conformance demonstration was not detailed enough to confirm conformance to 'should' clauses. It typically states, "The licensee complies with clause 6.2.4.2 of IEC 61513". There is evidence of some 'should' clauses being addressed (for example, 6.2.6.i). The analysis stops at the 6.x.x.x clause level (where x.x.x represents the numeric clause value such as clause 6.2.4.2). Note: many of the detailed requirements are in the lower level clauses (that is, clauses with nomenclature of the form 6.x.x.x.x). I raised my concern on the shortfall of coverage of IEC 61513 clauses with Westinghouse in RQ-AP1000-1707. 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. Westinghouse confirmed that the compliance assessment would be completed post-GDA as part of addressing existing assessment finding AF-AP1000-CI-005 (see Ref. 19). I have identified the need for the analysis to address all clauses including all 'should' and 'may' statements under the assessment finding below.

53. I queried the potential for Westinghouse to reconfigure the reactor coolant system hot leg temperature and steam generator level voting logic from (1oo2)x2 to 2oo4 (RQ-AP1000-1535). The advantage of using a 2oo4 architecture is that it has improved reliability and tolerance to faults than that provided by a (1oo2)x2 architecture. Two reactor coolant system sensors are provided in each of the two reactor coolant loops. There are also two steam generator level sensors provided for each of the two steam generators. The arrangement is such that the two sensors feeding the 1oo2 vote are connected to the same reactor coolant loop / steam generator. In this arrangement, reactor faults need to be sensed in both loops / steam generators before protective action is initiated. Changing the voting logic would potentially provide improved response to faults that initially appear in one reactor coolant loop/steam generator.

54. In response, Westinghouse provided a revision of Ref. 3 (Ref. 28), that describes, in the ALARP section, a potential improvement in relation to the reactor coolant system hot leg temperature voting logic (that is, a change from (1oo2)x2 to 2oo4 actuate logic). Westinghouse has not analysed the proposed change in detail for its impacts on the transient or safety analyses. Westinghouse is to make the change from (1oo2)x 2 to 2oo4 post-GDA, subject to confirmation that it does not have negative safety impacts such as unnecessary actuations. For the steam generator level voting logic, Westinghouse considered a number of options to determine the ALARP configuration. Westinghouse concluded that the ALARP solution is a change to 2oo4 voting logic from (1oo2)x2. I confirmed that Ref. 28 (safety plan, Table 4.1-1, requirements section) contains these commitments and consider it appropriate for them to be addressed post-GDA as the detailed design of the DAS is developed. If the proposed changes are implemented the DAS automatic functions will use either 2oo3 or 2oo4 voting logic.

55. I discuss my assessment of the key references to Ref. 3 (that is, Refs. 4, 5, 16 and 7) below.

56. Ref. 4 evaluates conformance of the DAS to those SAPs from Ref. 17 considered by Westinghouse to be appropriate for a Class 2 safety system. It provides a demonstration for each SAP, in a tabular CAE trail format, that the SAPs are met. I reviewed Ref. 4 and sampled a number of SAP CAE trails (see Ref. 20).

57. In the main, Ref. 4 met my expectations in terms of coverage of SAPs, for example, in relation to coverage of the safety system ESS SAPs (see Table 2-1 of Ref. 4). I raised a number of queries with Westinghouse in RQ-AP1000-1738, such as asking Westinghouse to:

- explain the small number of exceptions in terms of SAP coverage (EKP.5, EHF.7 and ERC.2);
- address shortfalls in coverage of evidence in the CAE trails;
- explain the approach to electrical isolation of data links between systems important to safety; and
- clarify the application of the SAPs to the 7300 series platform.

58. In response, Westinghouse clarified that the United Kingdom AP1000 Plant C&I Architecture SAPs Conformance Assessment (Ref. 29) addresses the SAP exceptions at the facility level. Westinghouse also provided additional evidence references in a revision of Ref. 4 (that is, Ref. 30) and committed to provide electrical isolation between the DAS and plant control system (PLS), recorded as a gap in the safety plan, Ref. 28, Table 4.1-1. Westinghouse explained how it applies the SAPs to the 7300 series platform.

59. I found that Ref. 5 provides an IEC 61508-2 compliance assessment for the UK DAS in support of Westinghouse's production excellence claim. Westinghouse proposed to revise Ref. 5 as the gap compensating measures are completed. I noted that, for 'shall' clauses, Westinghouse provided an argument, evidence trail and, where appropriate, a gap compensating measure. I raised generic issues relating to Westinghouse's approach to standards compliance demonstrations in RQ-AP1000-1707. Westinghouse's compliance demonstration considers 'should' and 'may' statements but does not identify gaps or compensating measures. As for the IEC 61513 conformance analysis, and 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. 19). I have identified the need for the analysis to address all clauses including all "should" and "may" statements under the assessment finding below.

60. In addition to the generic finding, I raised a number of specific queries (RQ-AP1000-1759 and RQ-AP1000-1783), such as Westinghouse to:

- clarity its intentions in regard to the use of a 'proven-in-use' case (see also AF-AP1000-CI-020, Ref 19, which states " … claims of proven-in-use / reliance on operating history are made explicit in the BSC");
- explain its approach to assessment of normative references, (that is, as presented in section 2 of IEC 61508-2);
- address the absence of an assessment of clause 4 (requirements for conformance to the standard), clause 5 (requirements for documentation) and clause 6 (management of functional safety); and
- define the content of the referenced implementation guides (such as, for control of DAS systematic and random hardware failures).

61. In response, Westinghouse clarified that they are not making a proven-in-use case for the UK **AP1000** reactor DAS system and application. The techniques and measures identified in IEC 61508-2 provide the basis of the approach for the systematic integrity demonstration of the complete system. Westinghouse intends to make a proven-in-use case for the 7300 series platform boards using data in Ref. 31. Westinghouse provided additional compliance statements addressing the identified gaps. For example,

Westinghouse clarified how they address management of functional safety and defined the content of the implementation guides. Westinghouse provided Ref. 32, a revision of Ref. 5, which includes changes outlined in the RQ responses.

62. The objective of Ref. 16 is to define the safety lifecycle for the DAS system design, hardware design and implementation to ensure the performance of activities needed to achieve and maintain the required safety integrity. In particular, Ref. 16 requires the performance of phases of the DAS safety lifecycle in accordance with IEC 61508-2 and IEC 61513.

63. I raised queries in relation to: the definition and use of requirements to ensure that adequate diversity is delivered (known as diversity-seeking decisions) by the design process (for example, to ensure diversity between the DAS and PMS); the definition of techniques and measures; and the planning of the functional safety assessment activity (RQ-AP1000-1725). Westinghouse's response provided the requested clarifications and a revision of Ref. 16 was submitted (Ref. 27). Westinghouse explained that the DAS system requirements specification would capture the diversity-seeking decisions. Ref. 27 includes the definition of the techniques and measures to be applied and notes that the functional safety assessment plan will be produced during the DAS planning phase.

64. Westinghouse letter WEC-REG-0328N NPP_JNE_000328 (Ref. 7) presents the DAS EQ approach. The DAS EQ programme is intended to provide assurance that the DAS is capable of meeting its functional and performance requirements while subject to specified environmental conditions (such as temperature, humidity and seismic conditions). Westinghouse state that the 7300 series based DAS for use in the UK **AP1000** plant shall be qualified in accordance with the **AP1000** plant EQ methodology (Ref. 24).

65. My review of Westinghouse's EQ submission identified a number of areas that needed further clarity, such as definition of functional requirements, use of representative configurations, impact of loss of the heating, ventilation and air conditioning system and approach to seismic qualification (that is, use of test and/or analysis techniques) (RQ-AP1000-1438, RQ-AP1000-1488, RQ-AP1000-1553 and RQ-AP1000-1759).

66. The responses to the RQs provided the requested clarifications. For example, Westinghouse explained that DAS EQ requirements will consider both normal and abnormal environmental conditions (RQ-AP1000-1759 response). The DAS equipment qualification programme is a representative type test that includes environmental testing and Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) susceptibility testing to ensure DAS operability during normal and abnormal conditions. The DAS is seismically tested, for example, to ensure that a squib valve is not spuriously actuated. Westinghouse does not undertake seismic testing of the DAS to ensure successful operation during or after abnormal seismic conditions (the PMS provides protection for such events). Westinghouse performs DAS functional testing for normal operating conditions during factory acceptance testing.

67. Westinghouse's justification for seismically qualifying the DAS to withstand a small earthquake event by analysis is contained in Ref. 3 (section 7). For example, Westinghouse explains they have previously qualified the 7300 series hardware by test to such levels, cabinets and sensors are similar to previously qualified and tested components and cabinet mounts are the same design as those used on seismically qualified and tested cabinets. The safety plan presented in Ref. 3 identifies the need for a detailed seismic assessment to be performed in line with IEC 60980 post-GDA.

68. The DAS cabinets contain temperature alarms that alert plant operators to abnormal temperatures. Westinghouse tests the DAS cabinets up to 120 degrees Fahrenheit to ensure that the DAS would not generate a spurious actuation signal upon heating,

ventilation and air conditioning system failure. I have raised GDA assessment finding CP-AF-AP1000-CI-001 below requiring the licensee to ensure the EQ programme addresses the UK specific EQ conditions, which should include consideration of the full impact of loss of the heating, ventilation and air conditioning system (for example, consideration of adverse humidity changes). Westinghouse confirmed its conformance to IEC 61000 (such as, for radiated emissions testing and CE mark certification). Westinghouse explained that DAS EQ tests will use a representative configuration of DAS cabinets containing every component of the DAS that requires qualification testing.

69. I confirmed that Ref. 28 and its supporting references adequately address the topics and elements of a BSC as outlined in the GDA issue and ONR GDA Issues Closure Guidance Document Ref. 21. The BSC identifies that Westinghouse uses IEC 61513 to implement the DAS safety life-cycle and IEC 61508-2 for the production excellence CAE. Westinghouse presented an equivalence argument to justify its use of IEC 61513 in preference to IEC 61508-1 for the implementation of the DAS safety lifecycle. The BSC draws on a SAPs conformance assessment (Ref. 30) that includes all relevant SAPs applicable to the DAS application and 7300 series platform. In addition, the ALARP assessment identifies relevant good practice applicable to DAS development and use of reliability assessments to inform the design. The BSC addresses Step 4 TOs and fulfils commitments contained in the Westinghouse resolution plan (for example, through submission of the BSC and supporting references).

70. Following assessment of Westinghouse's GDA issue action GI-AP1000-C&I-01.A2 submission of a DAS BSC, I am content that the BSC (Ref. 28), together with the supporting submissions, adequately address the GDA issue action. I have raised an assessment finding below to record those matters arising from the assessment that need to be addressed during the implementation of the DAS.

> GDA Assessment Finding: **CP-AF-AP1000-CI-001 –** The Licensee shall fully develop the safety case outlined in the DAS BSC as the detailed design of the DAS is completed post-GDA, and implement the BSC safety plan including:
>
> - document and justify the adequacy of the final DAS architecture and design in the safety case (that is, changes from (1oo2)x2 to 2oo4 as committed to in the BSC);
> - implement the compensating measures identified in the SAPs, IEC 61513 and IEC 61508-2 compliance assessments (for example, by including design and implementation detail, addressing all clauses and all 'should'/'may' statements within clauses);
> - ensure that the EQ programme addresses the detailed UK **AP1000** reactor DAS design and UK specific EQ conditions; and
> - implement the requirements of the DAS safety lifecycle document (for example, adequate coverage of diversity-seeking decisions in the DAS safety lifecycle and verification of lifecycle outputs).

For further guidance on the completion of the DAS safety case see TOs CI-01-TO2-2.2.2.2-1 to 10, CI-01-TO2-2.2.2.3-1, CI-01-TO2-2.2.2.4-1 and 2, CI-01-TO2-2.2.2.5-1, CI-01-TO2-2.2.2.6-1 to 3, CI-01.TO2-2.2.2.9-1 to 5, CI-02-TO2-3.1.3.1-1 and 2, and CI-02-TO2-3.2.2.3-1 in Ref. 20.

4.2.3 GDA Issue Action GI-AP1000-CI-02.A1 – Substantiation the Automatic DAS Remains in Service During Reactor Power Operation.

71. In this part of my assessment, I review Westinghouse's response to GDA issue action GI-AP1000-CI-02.A1. The GDA issue action requires Westinghouse to provide a substantiation that the automatic DAS remains in service during reactor power operation including during maintenance and proof testing. In response to this GDA action, Westinghouse has provided DAS architecture drawings (Ref. 10) and DAS functional logic diagrams (Ref. 11). I assessed the DAS architecture and logic drawings for provision of the automatic functions by a combination of (1oo2)x2 and 2oo3 voting (Ref. 20). I found the voting logic implements the automatic functions as either (1oo2)x2 or 2oo3. Further, Westinghouse has committed to change the (1oo2)x2 functions to 2oo4, dependent on the results of transient analysis to be undertaken post-GDA (see above).

72. The DAS architecture meets the objective sought by the GDA issue of ensuring that the DAS remains in service during maintenance or repair, and provides improved tolerance to single random hardware failures (for example, of an instrument or logic channel). The ability to remain in service is delivered by the additional redundancy provided (that is, over and above that present in the original 2oo2 architecture) and bypass facilities that support operational testing. As well as the redundancy provided by the input channels to the voting logic (for example, three channels feed into the 2oo3 voting logic) the DAS includes redundant voting logic, thereby permitting testing during power operation. The bypasses allow testing of DAS components without actuating output devices and maintain the ability to trip the reactor or actuate engineered safety features actuation system (ESFAS) on detection of safety demands.

73. I conclude GDA that issue action GI-AP1000-CI-02.A1 is closed by the Westinghouse submissions (Refs. 10 and 11). However, the licensee will need to confirm the adequacy of the final architecture (for example, following the transient analysis) as noted under the assessment finding above.

4.2.4 GDA Issue Action GI-AP1000-CI-02.A2 – Substantiation that the Automatic and Manual DAS meet their Reliability Targets

74. In this section I assess Westinghouse's response to GDA issue action GI-AP1000-CI-02.A2, which requires Westinghouse to provide a substantiation that the automatic and manual DAS meet their reliability targets. Refs. 8 and 9 provide the requested substantiation. I reviewed Ref. 9 and found Westinghouse uses a reliability block diagram methodology. The calculated reliability values are conservative since all failures are included, not just dangerous failures. Westinghouse made use of a commercially available tool (217Plus^{TM}) for generation of the reliability values. I found that the results of the analysis demonstrated that each of the DAS functions met Westinghouse's reliability target. However, the approach did not address the potential for common cause failure (CCF) of components, such as, the UPSs in the dual DAS power supply chain. In addition, the DAS UPSs use smart devices. I raised a number of queries with Westinghouse in RQ-AP1000-1612, RQ-AP1000-1638 and RQ-AP1000-1719. For example, Westinghouse to explain; the absence of CCF analysis, its approach to demonstrating that the UPSs are fit for purpose and how it maintains configuration control of the analysis.

75. Westinghouse provided a revision to Ref. 9 (that is, Ref. 33) and updated the DAS BSC safety plan (Ref. 28). I found that the responses to the RQs, Ref. 33 and Ref. 28 addressed my queries. For example, the DAS BSC safety plan in Ref. 28 includes a commitment to use the smart device process developed in response to GDA issue GI-AP1000-CI-05 for the assessment of the UPSs (see APP-GW-GEE-5328, Addition of Smart Device Identification and Justification Requirement for UK **AP1000**, Ref. 37). With regard to configuration control of the analysis, Westinghouse explained that the analysis was performed for the conceptual DAS design and that part revision numbers will be provided during the detailed DAS design phase when the reliability analysis

report is updated. In addition, Westinghouse's change control process addresses the impact of component changes on the veracity of the reliability analysis.

76. Ref. 33 includes consideration of CCF and demonstrates satisfaction of Westinghouse's unavailability target (less than 1.0E-2), with the exception of the manual ADS-4 and IRWST injection functions (1.0023E-02). Westinghouse needs to address improvements to the DAS to mitigate this concern when performing the detailed design (that is, to ensure the DAS meets its reliability targets for all safety functions). I found that Westinghouse is using unavailability as a surrogate for PFD and the figure includes all failures. Westinghouse needs to provide substantiation of the use of a 2% beta factor during the work to complete the IEC 61508-2 standards compliance demonstration and analyse the sensitivity to its variation. Westinghouse needs to develop the analysis to provide a PFd figure and demonstrate that it meets the 10-2 PFD target.

77. I also noted that the unavailability target for the five automatic function actuation cases presented in Ref. 33 is not satisfied during the actuation logic test. For example, (see Ref. 33 Table 6.1-5), during the short time (16 hours per year) of the actuation logic test, the pressuriser level low reactor trip and passive residual heat removal actuation function unavailability is 1.5317E-02 as compared to total function unavailability of 6.5449E-04 (that is, excluding contribution for power supply unavailability). Note that the actuation logic test reduces everything after the 2oo3 and (1oo2)x2 voters from two parallel paths to a single path. Westinghouse needs to consider any reasonably practicable improvements to the design (for example, use of higher reliability components) or testing arrangements to improve DAS reliability during maintenance periods.

78. The ONR PSA team confirmed that the PSA uses DAS function reliability figures consistent with the values calculated by Westinghouse (Ref. 26). However, the conceptual design of the DAS is the basis for the reliability analysis undertaken on the DAS (as documented in Ref. 33). The reliability analysis will need to be further developed post-GDA to address the detailed and as-built DAS design.

79. I reviewed the DAS FMECA documentation (Ref. 8) submitted by Westinghouse. I found that the approach adopted by Westinghouse includes a criticality analysis, which extends the classical FMEA by identifying the relative risk associated with each DAS element failure mode. The relative risk is a combination of consequence (criticality) and likelihood of occurrence. The approach undertaken by Westinghouse in performing the FMECA is consistent with industry practices.

80. Following my review of the FMECA, I raised a number of queries in RQ-AP1000-1639 and RQ-AP1000-1719. For example, the FMECA concludes that the design of the DAS is such that failures (such as power supply failures) tend to prevent actuation, not cause it. I queried why Westinghouse considered this the fail-safe state. Westinghouse has identified the means by which failures, such as power supply failures, would be detected (such as alarms in the PLS / data display and processing system). Westinghouse stated it is confident that the final design of the DAS will meet its reliability targets. Westinghouse also explained that the use of de-energise- to-actuate architecture would potentially increase the frequency of spurious reactor trips and ESFAS actuations (see Ref. 3). Given the DAS is a Class 2 system contributing to the achievement of Category A functions in combination with the PMS, I consider the argument presented by Westinghouse to be reasonable. I judge that the FMECA submitted by Westinghouse is satisfactory, given the current stage of DAS design.

81. Following assessment of Westinghouse's submissions in response to GDA issue action GI-AP1000-C&I-01.A1, on provision of substantiation that the automatic and manual DAS meet their reliability targets, I am content that the GDA issue action can

be closed. 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 DAS.

GDA Assessment Finding: **CP-AF-AP1000-CI-002 –** The Licensee shall:

- document and justify the reliability of the final detailed DAS design in the safety case;
- ensure the reliability analysis provides a PFD figure for each individual safety function and addresses all sources of random, common mode and systematic failures;
- improve the design and / or testing arrangements for the automatic safety functions to enhance DAS reliability during maintenance;
- update the overall **AP1000** plant PSA, as necessary, to reflect the final DAS detailed design reliability calculations; and
- review and revise the DAS FMECA once the detailed design is completed.

For further guidance on the completion of the DAS reliability substantiation, see TOs CI-02-TO2-3.2.2.1-1 to 6, CI-02-TO2-3.2.2.2-1 to 7 and CI-02-TO2-3.2.2.3-1 in Ref. 20.

4.2.5 Overall Conclusion on GDA Issues GI-AP1000-CI-01 and GI-AP1000-CI-02

82. I am content that an adequate position has been reached for all five actions and that GDA issues GI-AP1000-CI-01 and GI-AP1000-CI-02 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 case submissions (for example, update to the DAS BSC, Ref. 28). The safety case presented is adequate given the conceptual nature of the design and the further work required to complete the DAS design and implementation. In addition, Westinghouse has shown an increased understanding of the expectations for UK safety case documentation such as the DAS BSC and supporting submissions.

83. I have raised assessment findings above to record those matters arising from the assessment that need to be addressed post-GDA. These matters include the need for Westinghouse to fully develop and implement new processes that align with IEC nuclear standards for Class 2 equipment (that is, over and above those used for the standard **AP1000** plant C&I).

4.3 Comparison with Standards, Guidance and Relevant Good Practice

84. My assessment has included consideration of whether the Westinghouse submissions meet the expectations of relevant standards, guidance and good practice. I describe my assessment in the sections above (for example, assessment of SAPs CAE and IEC 61508-2 compliance submissions, Refs. 4 and 5). I am content that Westinghouse has made satisfactory use of relevant standards, guidance and good practice.

4.4 Assessment Findings

85. During my assessment two 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.

86. 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.

87. Residual matters are recorded as assessment findings if one or more of the following apply:

- Site-specific information is required to resolve this matter;
- the way to resolve this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter, requires licensee choices on organisational matters;
- to resolve this matter the plant needs to be at some stage of construction / commissioning; and
- to resolve this matter, the level of detail of the design needs to be beyond what can reasonably be expected in GDA (for example, manufacturer or supplier input is required; or areas where the technology changes quickly, and so to avoid obsolescence of design).

5 CONCLUSIONS

88. This report presents the findings of the assessment of GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0 DAS – Adequacy of Architecture relating to the UK **AP1000** plant GDA closure phase.

89. 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-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0 DAS – Adequacy of Architecture.

90. Overall, on the basis of my assessment, I am satisfied that GDA issues GI-AP1000-CI-01 and GI-AP1000-CI-02 can be closed.

6 REFERENCES

1. Office for Nuclear Regulation (ONR), ONR Guide NS-PER-GD-014 Revision 5, Purpose and Scope of Permissioning, August 2015 – TRIM 2015/304735.
2. Westinghouse Electric Company LLC, Resolution Plan for GI-AP1000-C&I-01 and GI-AP1000-C&I-02, DAS – Adequacy of Safety Case & Adequacy of Architecture – TRIM 2016/92069
3. Westinghouse Electric Company LLC, United Kingdom UK AP1000 Basis of Safety Case for the 7300 Series Diverse Actuation System - UKP-DAS-GLR-001, Rev. 1 – TRIM 2016/296907
4. Westinghouse Electric Company LLC, United Kingdom UK AP1000 Diverse Actuation System Safety Assessment Principle Compliance – UKP-DAS-GLR-005, Rev. 0 – TRIM 2016/296924
5. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System IEC 61508-2 Compliance – UKP-DAS-GLR-002, Rev. 0 – TRIM 2016/243574
6. Westinghouse Electric Company LLC, United Kingdom AP1000 7300 Series Based Diverse Actuation System Design Process – UKP-DAS-GEH-001, Rev. 1 – TRIM 2015/339839
7. Westinghouse Electric Company LLC, DAS Qualification Assessment – Westinghouse letter WEC-REG-0328N NPP_JNE_000328 – TRIM 2015/350760
8. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Failure Modes, Effects and Criticality Analysis – UKP-DAS-GLR-004, Rev. 0 – TRIM 2016/210157
9. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Reliability Analysis Report – UKP-DAS-GLR-003, Rev. 0 – TRIM 2016/210145
10. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Architecture Drawings UKP-DAS-J0-001, Rev. 0 (sheets 001 to 043) – TRIM 2016/127986
11. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Functional Logic Diagrams UKP-DAS-J3-001, Rev.0 (sheets 001 to 026) – TRIM 2016/127994
12. Westinghouse Electric Company LLC, Changes to Diverse Actuation System (DAS) Voting Logic and Associated Architecture – APP-GW-GEE-2286 – TRIM 2015/128080
13. Westinghouse Electric Company LLC, Changes to Diverse Actuation System (DAS) Platform Implementation – APP-GW-GEE-2287 – TRIM 2015/128084
14. Westinghouse Electric Company LLC, Modifications to Diverse Actuation System – APP-GW-GEE-3001 – TRIM 2015/346090
15. Westinghouse Electric Company LLC, Corrections to Power Sources for Diverse Actuation System, DCP APP-GW-GEE-4517 – TRIM 2015/346212
16. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Safety Lifecycle – UKP-DAS-GEH-001, Rev. 2 – TRIM 2016/225229
17. ONR, Safety Assessment Principles (SAPs) (www.onr.org.uk/saps/saps2014.pdf)
18. ONR, Permissioning Inspection – Technical Assessment Guides (www.onr.org.uk/operational/tech_asst_guides/index.htm)
19. ONR, Generic Design Assessment – New Civil Reactor Build: Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor – Assessment Report: ONR-GDA-AR-11-006. Rev. 0 – www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf

20. Altran UK Ltd, GI01 & GI02 Diverse Actuation System – Adequacy of Safety Case and Adequacy of Architecture – S.P1641.40.TSC267.1 – TRIM 2017/10136
21. ONR, C&I GDA Issues Closure Guidance Document, Rev. 0 – TRIM 2015/84414
22. ONR, C&I GDA Issues Closure Guidance Document Covering Letter – TRIM 2015/84411
23. ONR, RQ tracking Sheet – TRIM Ref 2016/383615
24. Westinghouse Electric Company LLC, AP1000 Equipment Qualification Methodology – APP-GW-G1-002, Rev. 4 – TRIM 2015/350769.
25. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Reliability Analysis Report – UKP-DAS-GLR-003, Rev. 1 – TRIM 2016/472090
26. ONR, ONR PSA Team confirmation that the PSA uses DAS function reliability figures – TRIM 2016/493292
27. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Safety Lifecycle – UKP-DAS-GEH-001 Rev 4 – TRIM 2016/482530
28. Westinghouse Electric Company LLC, United Kingdom UK AP1000 Basis of Safety Case for the 7300 Series Diverse Actuation System – UKP-DAS-GLR-001, Rev. 2 – TRIM 2016/484831.
29. Westinghouse Electric Company LLC, United Kingdom AP1000 Plant C&I Architecture SAPs Conformance Assessment – UKP-GW-GLR-039 Rev 0 – TRIM 2016/354451
30. Westinghouse Electric Company LLC, United Kingdom UK AP1000 Diverse Actuation System Safety Assessment Principle Compliance – UKP-DAS-GLR-005, Rev. 1 – TRIM 2016/482730.
31. Westinghouse Electric Company LLC, 7300 Process Protection and Control System Life Cycle Management Planning Sourcebook – WCAP-16673-P, Rev. 1 – TRIM 2015/479891
32. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System IEC 61508-2 Compliance – UKP-DAS-GLR-002, Rev. 1 – TRIM 2016/492519
33. Westinghouse Electric Company LLC, United Kingdom AP1000 Diverse Actuation System Reliability Analysis Report – UKP-DAS-GLR-003, Rev. 1 – TRIM 2016/472090
34. ONR, Assessment Report GDA Issue GI-AP1000-EE-01 – PCSR Presentation of Claims, Arguments and Evidence – TRIM 2016/274980
35. ONR, ONR Assessment Rating Guide – TRIM 2016/118638
36. ONR, Fault Studies Input to C&I Issues – DAS Voting Logic – TRIM 2016/8576
37. Westinghouse Electric Company LLC, APP -GW-GEE-5328, Addition of Smart Device Identification and Justification Requirement for UK, TRIM 2016/482388
38. ONR, ONR-GDA-AP-14-001 Rev. 0, AP1000 GDA C&I Assessment Plan, April 2015 – TRIM 2015/149263
39. Westinghouse Electric Company LLC, AP1000 Design Reference Point for UK GDA – UKP-GW-GL-060 Rev. 9 – TRIM 2016/446340
40. Westinghouse Electric Company LLC, AP1000 Pre-Construction Safety Report, UKP-GW-GL-793 Rev. 1, January 2017 – TRIM 2017/43700
41. ONR, ONR Assessment Report ONR-NR-AR-16-020 Internal Hazards GDA issues GI-AP1000-IH-01 to IH-06 – TRIM 2016/275001

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-001	The Licensee shall fully develop the safety case outlined in the DAS BSC as the detailed design of the DAS is completed post-GDA, and implement the BSC safety plan including: • document and justify the adequacy of the final DAS architecture and design in the safety case (that is, changes from (1oo2)x2 to 2oo4 as committed to in the BSC); • implement the compensating measures identified in the SAPs, IEC 61513 and IEC 61508-2 compliance assessments (for example, by including design and implementation detail, addressing all clauses and all 'should'/'may' statements within clauses); • ensure that the EQ programme addresses the detailed UK **AP1000** reactor DAS design and UK specific EQ conditions; and • implement the requirements of the DAS safety lifecycle document (for example, adequate coverage of diversity-seeking decisions in the DAS safety lifecycle and verification of lifecycle outputs). For further guidance on the completion of the DAS safety case see Technical Observations (TOs) CI-01-TO2-2.2.2.2-1 to 10, CI-01-TO2-2.2.2.3-1, CI-01-TO2-2.2.2.4-1 and 2, CI-01-TO2-2.2.2.5-1, CI-01-TO2-2.2.2.6-1 to 3, CI-01.TO2-2.2.2.9-1 to 5, CI-02-TO2-3.1.3.1-1 and 2, and CI-02-TO2-3.2.2.3-1 in Ref. 20.	4.2.2
CP-AF-AP1000-CI-002	The Licensee shall: • document and justify the reliability of the final detailed design in the safety case; • ensure the reliability analysis provides a probability of failure on demand (PDF) figure for each individual safety function and addresses all sources of random, common mode and systematic failures; • improve the design and/or testing arrangements for the automatic safety functions to enhance DAS reliability during maintenance; • update the overall **AP1000** plant PSA, as necessary, to reflect the final DAS	4.2.4

	detailed design reliability calculations; and • review and revise the DAS FMECA once the detailed design is completed. For further guidance on the completion of the DAS reliability substantiation see TOs CI-02-TO2-3.2.2.1-1 to 6, CI-02-TO2-3.2.2.2-1 to 7 and CI-02-TO2-3.2.2.3-1 in Ref. 20.	