New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issues GI-AP1000-FS-03 “Diversity for Frequent Faults” and GI-AP1000-FS-04 “Provision of Enhanced and Diverse Flux Protection to Protect against Adverse Power Distribution Faults”

Assessment Report: ONR-NR-AR-16-024
Revision 0
March 2017

Published 03/17

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

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

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses two closely related GDA Issues:

- GI-AP1000-FS-03 – Diversity for Frequent Faults
- GI-AP1000-FS-04 – Provision of Enhanced and Diverse Flux Protection to Protect against Adverse Power Distribution Faults

These GDA Issues arose in GDA Step 4 due to the long-established practice in the UK of demonstrating diversity of protective measures for frequent design basis faults (initiating event frequencies of greater than 1×10^{-3} per year). Westinghouse initiated a package of work to demonstrate that for a large number of design basis faults the **AP1000** reactor does have 'primary' and 'diverse' back-up means of providing necessary safety functions. However, by the end of GDA Step 4, ONR was not satisfied with the completeness of this demonstration, in particular for faults associated with changes in neutron flux. The seven actions of GI-AP1000-FS-03 were written with the objective of ensuring that Westinghouse could systematically close the gaps identified by ONR through a combination of further safety case analysis and documentation, and if appropriate and reasonably practicable, by modifications to the plant.

At the time of writing the GDA Issues, ONR envisaged that to fully demonstrate diversity of safety protection for frequent reactivity faults, enhancements to the flux monitoring and protection systems would be needed. The original safety case claimed the ex-core flux detection as part of the protective measures for these types of faults, but no claims were made on the in-core detectors already included within the design to support normal operation. ONR anticipated that a likely outcome of GI-AP1000-FS-03 would be the need for additional flux protection in fault conditions and enhancements to the in-core detection as potentially effective ways to provide that protection. Therefore, the two actions of GI-AP1000-FS-04 formalised the requirement for Westinghouse to review the adequacy of the **AP1000**'s flux protection and consider if improvements to the in-core flux detection were among the reasonably practicable options.

Sensibly, Westinghouse chose to address GI-AP1000-FS-03 and GI-AP1000-FS-04 with a consolidated approach. This is reflected in ONR's assessment and this combined assessment report covering both GDA Issues.

The requirements of the GDA Issue actions were significant and wide ranging, for which Westinghouse has needed to undertake (and document) a significant amount of transient analysis, optioneering studies, and safety case justifications.

- For GI-AP1000-FS-03 Action 1, Westinghouse has repeated some GDA Step 4 analyses of Anticipated Transients Without Scram (ATWS) events, using its latest computer models and design reference point to show that its safety case conclusions asserted before the pause remain valid.
- For GI-AP1000-FS-03 Action 2, Westinghouse has analysed additional and more severe excessive increase in steam removal faults to show that no enhancements to the **AP1000** design are required in order to meet UK expectations for frequent faults.
- For GI-AP1000-FS-03 Action 3, Westinghouse has analysed rod cluster control assembly drop faults, assuming the primary protective measures claimed in the safety

case are unavailable, to show that no enhancements to the **AP1000** design are required in order to meet UK expectations for frequent faults.

- For GI-AP1000-FS-03 Action 4, Westinghouse has provided evidence that a modification to the **AP1000** design identified and credited in the analysis during GDA Step 4 has been fully integrated into the safety case and design documentation.
- For GI-AP1000-FS-03 Action 5, Westinghouse has reanalysed complete loss of reactor coolant pump faults assuming the initial conditions are perturbed to the extremes of the grid frequency ranges required by the UK grid code. By doing this, it has shown that its previously stated safety case claims assuming nominal conditions remain valid and no enhancements to the **AP1000** design are required in order to meet UK expectations for frequent faults.
- For GI-AP1000-FS-03 Actions 6 and 7, Westinghouse has considered and analysed the consequences of Chemical and Volume Control System (CVS) failures during shutdown modes of operation. It has identified the need for a design change to meet UK expectations for frequent faults, proposing to include additional diverse flux protection in the form of automatic Core Makeup Tank (CMT) actuation and dilution source isolation initiated from the Diverse Actuation System (DAS).
- Taking cognisance of the work done for GI-AP1000-FS-03, for the two actions for GI-AP1000-FS-04 Westinghouse has systematically considered a range of potential improvements to the way the **AP1000** design detects reactivity and power distribution faults, including but not limited to enhancements to the in-core flux detection system. Ultimately, it has concluded that the only change that is reasonably practicable is the DAS automatic CMT actuation and dilution source isolation identified for GI-AP1000-FS-03 Actions 6 and 7.

Following a detailed review of Westinghouse's submissions, multiple meetings and discussions over several months, consultations with colleagues in other disciplines and through the issuance of regulatory queries to obtain further information, I am satisfied that:

- Westinghouse has undertaken all the necessary work required by the two GDA Issues;
- a modification is required to provide diverse protection for CVS failures in certain shutdown modes of operation;
- Westinghouse has generally been able to show that the **AP1000** reactor can meet the UK expectations for frequent faults without improvements to its flux protection systems; and
- it is not reasonably practicable to make further enhancements to the **AP1000**'s flux protection system, including the modifications to the extant in-core flux measurement system identified by ONR in GDA Step 4 as a potential option.

No new matters have arisen for a future licensee to consider and take forward outside GDA as a result of my assessment of GI-AP1000-FS-03 and GI-AP1000-FS-04.

In summary, I am satisfied that GDA Issues GI-AP1000-FS-03 and GI-AP1000-FS-04 can be closed.

LIST OF ABBREVIATIONS

3D-FAC	Three-Dimensional Final Acceptance Criteria
ALARP	As Low As Reasonably Practicable
AC	Alternating Current
ADS	Automatic Depressurisation System
AFCAP	Advanced First Core Program
AOO	Anticipated Operational Occurrence
ATWS	Anticipated Transients Without Scram
ATWT	Anticipated Transients Without Trip
BOC	Beginning of Cycle
C&I	Control and Instrumentation
CCF	Common Cause Failure
CIRT	Critical Issue Resolution Team
CMT	Core Makeup Tank
CVS	Chemical and Volume Control System
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DCP	Design Change Proposal
DNBR	Departure from Nucleate Boiling Ratio
DWS	Demineralised Water Transfer and Storage System
EOC	End of Cycle
EPRI	Electric Power Research Institute
FON	Fraction of Normal (full power flux)
GDA	Generic Design Assessment
GRCA	Grey Rod Control Assembly
GRS	Gesellschaft fur Anlagen und Reaktorscherheit
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IRWST	In-containment Refuelling Water Storage Tank
LOCA	Loss of Coolant Accident
MFWP	Main Feedwater Pump
MTC	Moderator Temperature Coefficient
ONR	Office for Nuclear Regulation
PCI	Pellet-Clad Interaction

PCSR	Pre-Construction Safety Report
PLS	Plant Control System
PMS	Protection and Monitoring System
PORV	Power-Operated Relief Valve
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System
SAC	Safety Analysis Checklist
SAPs	Safety Assessment Principles
TSC	Technical Support Contractor
US NRC	United States Nuclear Regulatory Commission
VFD	Variable Frequency Drive
WENRA	Western European Nuclear Regulators Association

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

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

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses two closely related GDA Issues:

   - GI-AP1000-FS-03 – Diversity for Frequent Faults
   - GI-AP1000-FS-04 – Provision of Enhanced and Diverse Flux Protection to Protect against Adverse Power Distribution Faults

3. The related GDA Step 4 report (Ref. 1) 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 Overview of GI-AP1000-FS-03 and GI-AP1000-FS-04

4. The **AP1000** reactor has been designed with a consideration of design basis events, defence-in-depth and utilising insights from Probabilistic Safety Analysis (PSA), all of which are consistent with relevant international good practice. However, early on in the original GDA fault studies interactions with ONR, Westinghouse was challenged to review all design basis initiating events with a frequency of greater than 1×10^{-3} per year and to demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each nuclear safety key function (eg reactivity control and fuel cooling). The demonstration of diversity for frequent design basis faults is long-established relevant good practice in the UK and has also been required from all the recent requesting parties submitting reactor designs for GDA determinations.

5. This challenge was captured through the regulatory observation RO-AP1000-47. In its response to the regulatory observation (Ref. 2), Westinghouse produced a matrix table in which each of the frequent design basis initiating faults was listed against a series of safety functions for the reactor and the spent fuel pool. For each frequent fault, Westinghouse claimed to have identified a 'primary' and a 'diverse' back-up means of providing the necessary safety functions.

6. Ref. 2 was assessed in detail by ONR during GDA Step 4 (see Ref. 1). In many cases, Westinghouse's arguments were accepted. However, in a number of cases ONR's judgement was that Westinghouse's demonstration of diversity was only partial or not convincing. The response to RO-AP1000-47 was received and assessed late on in GDA Step 4 and there was insufficient time for Westinghouse to address ONR's feedback. As a result, GDA Issue GI-AP1000-FS-03 (Ref. 3) was written requiring Westinghouse to complete this demonstration of diversity through a combination of analysis and (if necessary) design changes.

7. The majority of the events where outstanding work was required are associated with changes in neutron flux that can potentially challenge fuel safety limits. These types of events can be characterised into two groups:

- events that result in an increase in core heat removal
- events that result in reactivity and power distribution anomalies

8. GI-AP1000-FS-03 has seven actions to address the gaps identified by ONR, including one action (Action 4) to implement a design change already identified by Westinghouse (and welcomed by ONR) to improve the diverse Control and Instrumentation (C&I) protection available for an uncontrolled withdrawal of a Rod Cluster Control Assembly (RCCA) bank power fault when the reactor is at power.

9. Prominent among ONR's concerns set out in Ref. 1 was the apparent reliance of the **AP1000** design on the primary C&I Protection and Monitoring System (PMS) and the ex-core flux detectors. By the end of GDA Step 4, Westinghouse had not demonstrated to ONR's satisfaction what the safety case would be for many of the identified frequent reactivity faults should a coincident common cause failure (CCF) occur in either the PMS or the ex-core detectors. ONR's fault studies assessors were aware that other Pressurised Water Reactor (PWR) designs have taken credit for diverse in-core flux detectors in their safety cases for equivalent faults. The assessors were also aware that the **AP1000** design includes in-core detectors to provide inputs to a computer-based core monitoring system (called BEACON^{TM}) which supports normal operation. ONR accepted Westinghouse's position that the extant BEACON system was not suitable (for several reasons) to provide adequate protection for fast-acting reactivity transients but requested through Action 1 of GDA Issue GI-AP1000-FS-04 (Ref. 4) that Westinghouse examine the feasibility of enhancing the existing in-core instrumentation that is used by BEACON to improve the flux protection included within the plant design. In a second action, GI-AP1000-FS-04 required Westinghouse to demonstrate diverse protection for frequent reactivity and power distribution faults, potentially by claiming enhanced in-core instrumentation.

10. A summary of the requirements of each individual action is provided in Annex 1. The full requirements are set out in Refs 3 and 4.

11. Both GDA Issues gave Westinghouse the flexibility to address the intent of the original actions by alternative means. Westinghouse has chosen to consolidate its considerations and responses to several of the GI-AP1000-FS-03 actions with its response to the two actions on GI-AP1000-FS-04. I consider this to be a sensible and pragmatic approach. I have effectively adopted a similar approach, and as result this single assessment report captures my assessment of both GDA Issues.

1.3 Scope

12. The scope of this assessment is detailed in the assessment plan (Ref. 5). Consistent with this plan, the assessment is restricted to considering whether Westinghouse's submissions to ONR for GI-AP1000-FS-03 and GI-AP1000-FS-04 provide an adequate response to justify the closure of the GDA Issues and their associated actions. As such, this report only presents the assessment undertaken as part of the resolution of the two GDA Issues and it is recommended that this report be read in conjunction with the Step 4 fault studies assessment of the Westinghouse **AP1000** reactor (Ref. 1) in order to appreciate the totality of the assessment of the evidence on design basis reactor faults and the demonstration of diversity for frequent faults provided as part of the GDA process.

13. Any evaluation of reactor reactivity transients requires sophisticated methodologies and computer codes. In both its original safety case submissions (provided during GDA Steps 3 and 4) and its responses to these two GDA Issues, Westinghouse has supported its safety case claims with transient analysis undertaken with codes such as LOFTRAN, FACTRAN, VIPRE-01 and ANC. As part of its GDA Step 4 assessment (Ref. 1), ONR sampled several of Westinghouse's key computer codes to draw wider (generally positive) conclusions about the full suite of computer codes referenced by

the **AP1000** safety case. As a result, this assessment of the two GDA Issues has assumed that Westinghouse's methodologies and computer codes are adequate for the purposes identified and it does not attempt to repeat the Step 4 assessments.

14. As part of a separate fault studies GDA Issue (GI-AP1000-FS-02, Ref. 6), Westinghouse is required to demonstrate that all of its transient analyses submitted to ONR are appropriate for the declared design reference point. The adequacy of Westinghouse's response to GI-AP1000-FS-02, which needs to include within its scope analysis undertaken for GI-AP1000-FS-03 and FS-04, is reported separately.

15. The design changes identified for GI-AP1000-FS-03 Action 4 had already been considered and welcomed by ONR in GDA Step 4. Therefore the assessment in this report has not repeated earlier considerations on the merits of including such a modification within the design. Instead this assessment has focused on:

- the evidence that the change is reflected in the latest safety case documentation (notably Chapters 8 and 9 of the Pre-Construction Safety Report, PCSR);
- gaining an understanding about the extent to which the design details of the modification are being developed during GDA; and
- coming to a view on the adequacy of Westinghouse's processes to capture those commitments and functional requirements that will be addressed by future detailed design work and not during GDA.

16. It is important to note that this examination of Westinghouse's design change processes has been very limited and does not constitute a repeat of the assessment undertaken during GDA Step 4 as part of the management of safety and quality assurance (Ref. 7).

1.4 Method

17. This assessment has been undertaken consistent with internal guidance on the mechanics of assessment within ONR (Ref. 8).

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

18. ONR's GDA guidance to requesting parties (Ref. 9) states that the information required for GDA may be in the form of a PCSR, and the Technical Assessment Guide NS-TAST-GD-051 sets out regulatory expectations for a PCSR (Ref. 10).

19. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 11) 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.

20. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, and therefore this report does not attempt to assess the totality of the **AP1000** PCSR chapters related to fault studies (Chapters 8 and 9). However, a key aspect of this assessment has been to look at how the work undertaken for these two GDA Issues has been integrated and summarised in the PCSR. For example, evidence that the modification to the diverse C&I protection for an uncontrolled withdrawal of an RCCA bank power is reflected in the PCSR is a requirement for closure of GI-AP1000-FS-03 Action 4. Therefore, in various places in this assessment report I have commented on the adequacy with which the PCSR (especially Chapters 8 and 9) captures the safety case arguments or informs my conclusions.

2.2 Standards and Criteria

21. The assessment has been undertaken in line with the requirements of the HOW2 BMS document NS-PER-GD-014 (Ref. 12). In addition, the Safety Assessment Principles (SAPs, Ref. 13) constitute the regulatory principles against which dutyholders' safety cases are judged, and therefore they are the basis for ONR's nuclear safety assessment. The SAPs 2014 Edition (Revision 0) has been used when performing the assessment described in this report (the original GDA Step 4 fault studies assessment used the 2006 Edition).

2.2.1 Safety Assessment Principles and Technical Assessment Guides

22. The following SAPs (Ref. 13) were identified in the assessment plan (Ref. 5) as being appropriate to judge the adequacy of the arguments in the area of fault studies for the UK **AP1000**:

- Fault Analysis SAPs FA.1 to FA.9
- Severe Accidents SAPs FA.15 and FA.16
- Engineering SAPs EKP.2 to EKP.5, ECS.1, ECS.2, EDR.1 to EDR.4, ESS.2, ESS.4, ESS.6 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4
- Computer Codes and Calculation Methods SAPs AV.1 to AV.8
- Numerical Target for DBA Consequences Target 4

23. It is important to note, however, that the scope of the assessment to close out the GDA Issues is narrowly defined and is less than that of a typical ONR assessment, such as that undertaken in GDA Step 4. The original fault studies assessment (Ref. 1), which resulted in GI-AP1000-FS-03 and GI-AP1000-FS-04, considered the SAPs identified above. The objective of this assessment is primarily to judge the adequacy with which Westinghouse's submissions address the requirements of the GDA Issues rather than to repeat the original assessment against the SAPs.

24. Towards the end of this assessment, I have needed to balance the requirements of two different engineering SAPs (ESS.7 and ESS.18) because through meeting one of

them, a design change proposed by Westinghouse is challenging the other. This is discussed further in Section 4.7.

2.2.2 National and International Standards and Guidance

25. There are both International Atomic Energy Agency (IAEA) standards (Ref. 14) and Western European Nuclear Regulators Association (WENRA) reference levels (Ref. 15) that are relevant to the fault studies assessment of the **AP1000**. The original GDA fault studies assessment undertaken during Steps 3 and 4 took cognisance of the international standards published at the time. The GDA Issues that emerged from that original assessment can generally be characterised as having their origins in the application of the SAPs and UK relevant good practice rather than through the comparison against international guidance. Therefore, the SAPs (and not the international references) are the foremost standards considered. It should be noted that the latest version of the SAPs (Ref. 13) were benchmarked against the extant IAEA and WENRA guidance in 2014.

2.3 Use of Technical Support Contractors (TSCs)

26. No TSCs have been used directly in support of this assessment. As part of the work to close out GI-AP1000-FS-02, ONR placed a contract with the German company Gesellschaft fur Anlagen und Reaktorscherheit (GRS) to review the applicability of Westinghouse's updated analyses to the latest declared **AP1000** design reference point. Some of the findings of this work (Ref. 16) have been used to inform this assessment.

2.4 Integration with Other Assessment Topics

27. 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. The following cross-cutting issues have been considered within this assessment:

- The design change identified by Westinghouse as part of the response to GI-AP1000-FS-03 Action 4 is to the diverse C&I protection system (called the Diverse Actuation System, or DAS). Westinghouse has proposed further changes to the DAS as an outcome of its work to address Actions 6 and 7 of the same GDA Issue, and GI-AP1000-FS-04. The totality of the DAS design for the UK **AP1000** reactor is subject to several C&I GDA Issues, including GI-AP1000-CI-01, -02, and -03 (Refs 17, 18 and 19). As a result, I have consulted ONR's C&I assessors looking at these broader GDA Issues to seek their opinion on the adequacy of the modification and to determine if there are any implications for or from the wider work on the DAS.
- GI-AP1000-FS-03 Action 5 requires Westinghouse to consider the effects of grid frequency perturbations on loss of forced flow faults. The UK grid code establishes requirements for electricity generating units, including frequency variations the plant must be able to survive without tripping offline. There is an electrical engineering GDA Issue, GI-AP1000-EE-01 (Ref. 20), requiring Westinghouse to present claims, arguments and evidence for the **AP1000** electrical system in the PCSR. An ability to safely operate within the limits established by the UK grid code is a key claim that needs to be established and substantiated as part of the work to close GI-AP1000-EE-01. I have therefore consulted with my electrical engineering colleagues to ensure that Westinghouse has correctly interpreted the requirements of the UK grid code for GI-AP1000-FS-03 Action 5 and to advise them on the extent to which the fault studies work for this action can provide substantiation to the claims, arguments and evidence required for GI-AP1000-EE-01.

- At the time the requirements of GI-AP1000-FS-04 were written, it was anticipated that improvements to in-core flux detectors used to support normal operation through the BEACON code could help to provide some of the required diversity in flux measurement. A separate GDA Issue was raised in the fuel design area (GI-AP1000-FD-03, Ref. 21) to identify the processes in which BEACON contributes to nuclear safety and any hazards that could arise if the BEACON software failed in some way. It was therefore necessary during the course of the assessment of GI-AP1000-FS-04 and GI-AP1000-FD-03 to keep the role of BEACON under review because any modifications identified for the former GDA Issue could have implications for the scope of the latter. Ultimately, Westinghouse has not identified any changes to the requirements or role for the in-core detectors and BEACON to address GI-AP1000-FS-04.

2.5 Out of Scope Items

28. As has already been stated, this assessment has not attempted to revisit the original GDA Step 4 assessment of Westinghouse's methodologies or computer codes for analysing transients associated with changes in neutron flux.

29. The main safety criteria of interest for most of the events considered in this assessment are the margins to departure from nucleate boiling / critical heat flux and fuel centre line temperature. However, Westinghouse has not discussed the phenomenon of Pellet-Clad Interaction (PCI) in its submissions and it has not been discussed extensively in this assessment. PCI occurs when irradiated fuel pellets swell to put a tensile stress on a fuel pin's cladding. This can lead to stress corrosion-induced failures, notably following rapid power transients.

30. During GDA Step 4, Westinghouse responded to a regulatory observation on PCI with a report setting out the limits it would apply to the **AP1000** reactor to protect against the phenomenon and the '3D FAC' (three-dimensional final acceptance criteria) methodology it has developed to ensure that these limits are complied with (Ref. 62). This methodology was assessed at the time and judged to be acceptable (Ref. 53). Therefore, consistent with my general aim of not repeating assessments undertaken during GDA Step 4, I have not attempted to look again at this topic, especially given that the GDA Issues are primarily concerned with the diverse protection available for frequent faults in the unlikely event of the primary protection failing. Given the low frequency of the sequences considered in this assessment and the relatively small radiological consequences of PCI failures, the provision of further protection in addition to that considered during Step 4 is not something I have chosen to pursue.

31. The one exception to this approach on PCI is for RCCA misalignment faults (Section 4.3). During GDA Step 4, Westinghouse postponed the application of its PCI methodology to frequent RCCA misalignment faults until site licensing. I sought some additional assurances on the safety case strategy in this area as part of my assessment of GI-AP1000-FS-03 Action 3 (see Section 4.3).

3 REQUESTING PARTY'S DELIVERABLES IN RESPONSE TO THE GDA ISSUES

32. To address these two GDA Issues, Westinghouse initiated a significant amount of transient analysis, optioneering studies and safety documentation authoring. Westinghouse communicated progress on this wide-ranging study to ONR through regular meetings, but ultimately it consolidated its work into a number of key submissions.

33. The main report provided for GI-AP1000-FS-03 is "UK AP1000 Plant: Summary Report Supporting the Closure of the Fault Studies Issue 03" (Ref. 22). This report summarises the following:

- In response to Action 1, sensitivity analyses of a selection of Anticipated Transients Without Trip (ATWT) to show that cases previously analysed in GDA Step 4 (ie circa 2010) remain appropriate for the latest UK design reference point (Ref. 23).
- In response to Action 2, discussion of various postulated events that could result in increase in secondary steam flow faults and analyses of those events identified as bounding, assuming a common mode failure of the PMS and no reactor trip.
- In response to Action 3, discussion and analyses of a range of RCCA misalignment events to show that, even without a reactor trip and rod withdrawal block functions credited, appropriate safety criteria can be met.
- In response to Action 5, the frequency range established by the UK grid code and analyses to show that appropriate safety criteria can be met if a complete loss of flow fault occurs following a grid perturbation.
- In response to Action 7, analysis of boron dilution faults during shutdown conditions assuming a common mode failure of the PMS. The functional requirements for an identified design change to the DAS are identified as a result of this analysis.

34. Westinghouse supported its submission of Ref. 22 with six calculation notes which provide more details on the analyses described and presented (Refs 24, 25, 26, 27, 28 and 29).

35. Westinghouse addressed Action 4 outside Ref. 22. To show that it had incorporated the design change to the DAS to improve the protection for at-power uncontrolled withdrawal of an RCCA bank fault, Westinghouse supplied the Design Change Proposal (DCP) "DAS PRHR Logic Change" APP-GW-GEE-1481 (Ref. 30). This DCP was written in 2010 (ie during GDA Step 4 and prior to Westinghouse pausing its UK activities) and has been applied to the standard **AP1000** plant (ie it is a change not restricted to the UK). However, on its own, this DCP did not provide ONR with adequate information or evidence on how this change had been implemented into the UK safety case documentation and design. Of particular concern was the fact that the design for the DAS for the UK **AP1000** reactor will be different from that for the standard plant as a result of commitments made during GDA Step 4 and ongoing work to address GI-AP1000-CI-01 and GI-AP1000-CI-02 (Refs 17 and 18). Therefore, Westinghouse supplemented the DCP with an explanatory note setting out how the modification has been (or will be) implemented in the UK (Ref. 31).

36. In part due to ONR's queries on Action 4, but also as a result of similar questions for GI-AP1000-FS-01, Westinghouse made a number of presentations to ONR on its processes for design changes. ONR's assessment of these processes is described in Ref. 32.

37. To address Action 6 of GI-AP1000-FS-03, Westinghouse produced a standalone report "AP1000 Plant Chemical and Volume Control System (CVS) – Diversity Evaluation" (Ref. 33). This report (which completely supersedes an earlier submission,

Ref. 34) describes the various **AP1000** systems available to borate the Reactor Coolant System (RCS), summarises the reactivity control requirements in different operating modes, and then identifies and analyses two scenarios (classified as frequent faults) where extra design provision could be merited to protect against CVS failures. A number of possible design changes are considered and ultimately one modification is recommended. This design change is the same as that identified for Action 7 in Ref. 22.

38. To address the two actions of GI-AP1000-FS-04, Westinghouse produced an additional standalone report "AP1000 Flux Protection and Diversity for Frequent Faults" (Ref. 35). As originally written, ONR's GDA Issue assumed that a solution based on the in-core detectors used to support normal operations would have a role to play in any enhancements to the extant flux protection available for frequent reactivity faults. However, Ref. 35 takes a step back from this starting place by discussing all the frequent events that could generate severe changes in neutron flux (ie events that result in an increase in core heat removal or that result in reactivity and power distribution anomalies) and then considers a wide range of potential improvements which could provide diverse overpower / flux protection. In-core detectors are only one of the options Westinghouse has considered. With references to the analyses undertaken for GI-AP1000-FS-03 (Ref. 22), it concludes that the only reasonable practicable change is to connect the intermediate range ex-core detectors to the DAS. This will allow the Core Makeup Tanks (CMTs) to automatically add borated water into the RCS following certain fault conditions occurring in some shutdown modes (namely, those considered in Actions 6 and 7 of GI-AP1000-FS-03).

39. To implement this design change and to ensure that it is included with the UK **AP1000** design, Westinghouse has produced DCP APP-GW-GEE-5251 (Ref. 36). As well as identifying the need for the change to the DAS and being the vehicle by which the change gets included into the formal UK design reference (Ref. 23), it gives specific information on the nature of the changes proposed to the UK C&I architecture.

40. Throughout the assessment period during which time ONR was interacting with Westinghouse on these two GDA Issues, Westinghouse was updating the March 2011 PCSR (Ref. 37). To facilitate early closure of these two GDA Issues (ahead of a consolidated update to the PCSR being provided), Westinghouse provided a revised draft of PCSR Chapter 9 (Ref. 38) to show how it intends to incorporate the results of its work into the top-tier safety case documentation. It also supplied an updated version of Chapter 8 (from that included in Ref. 37) which includes a revised fault schedule for the **AP1000** reactor (Ref. 39), including revised entries for reactivity faults.

4 ONR ASSESSMENT OF GDA ISSUES GI-AP1000-FS-03 AND GI-AP1000-FS-04

41. My assessment of Westinghouse's submissions for GI-AP1000-FS-03 and GI-AP1000-FS-04 is set out below, against the scope defined in Section 1 and the strategy discussed in Section 2.

42. I have discussed the GI-AP1000-FS-03 actions in turn. For each, I have started by providing some additional background information to supplement that already provided in Sections 1 to 3 to give additional context. I have then detailed my assessment. As a result of their close relationship, I have considered Actions 6 and 7 together.

43. As originally written, GI-AP1000-FS-04 had two actions. Westinghouse has consolidated its response for the two actions and I have adopted a similar approach for my assessment. After some initial background information, I have split my assessment of GI-AP1000-FS-04 into two. First I have considered the adequacy of Westinghouse's submission, which recommends a design change. I have then moved on to discuss the adequacy with which Westinghouse has taken forward the identified design change and included it within the UK **AP1000** design.

4.1 GI-AP1000-FS-03 Action 1

4.1.1 Background

44. The need to demonstrate diversity for protecting against frequent design basis faults is largely a UK-specific expectation. However, one aspect of this expectation, the need to show that there is an alternative means to trip the reactor in a fault condition, is widely followed internationally, including by Westinghouse in its original analyses to support the **AP1000**. The requirement to consider and make design provision for so-called 'Anticipated Transients Without Scram' (ATWS) or 'Anticipated Transients Without Trip' (ATWT) in the US (the regulatory regime in which the **AP1000** design was developed) is set out in Ref. 40.

45. Having already considered such ATWS events as part of the design, Westinghouse was in a good starting position in GDA Step 4 to meet this aspect of the UK requirements. However, there are some notable differences between the US regulations and the UK expectations:

- The US ATWS regulations (Ref. 40) require the Anticipated Operational Occurrences (AOOs) to be considered with a failure to trip the reactor. AOOs are a category of reactor faults that are broadly equivalent to the frequent faults normally considered in the UK, but the mapping across is not absolute. In GDA Step 4 it was necessary for Westinghouse to review the completeness of its standard list of ATWS events for the UK and assess for the first time additional scenarios.

- There are three ways an ATWS could occur:
    1. a common mode failure in the C&I protection system which normally detects a problem and initiates a reactor shutdown (in the case of the **AP1000**, the PMS);
    2. a common mode failure of the reactor trip breakers which prevents a reactor trip despite a PMS signal; and
    3. a common mode mechanical fault which affects all and prevents the insertion of the RCCAs into the core. All PMS and DAS logic functions (with the exception of actually inserting RCCAs) will continue to be operable.

  Westinghouse had considered the first two as part of normal US practice, but it had not previously considered the third scenario.

- Although there is a requirement to consider ATWS events in the US, it is not a design basis requirement. This has implications for the level of conservatism assumed in the analysis, the safety criteria the analysis has to meet and, crucially for this GDA Issue action, what limits and conditions are identified from the analysis that need to be complied with during operation.

46. As a result of these differences, during GDA Step 4 Westinghouse performed a new set of ATWS evaluations for the UK (Ref. 41) using the latest computer models and design reference point established circa 2010. ONR broadly welcomed this analysis (see Ref. 1). However, consistent with SAP FA.9, a need for Westinghouse to identify key limits and conditions from this design basis analysis was identified. In particular, a set of reactivity parameters, including Moderator Temperature Coefficients (MTCs), relevant to the analysis of these faults, needed to be defined.

47. During GDA Step 4, discussions with Westinghouse established that it already maintains a document for the **AP1000** reactor called the Safety Analysis Checklist (SAC). The objective, status and revision of the SAC for the UK are the subjects of a separate fault studies GDA Issue, GI-AP1000-FS-02 (Ref. 6). In brief, it captures data generated by core design, fuel rod design and thermal hydraulic design basis safety evaluations during the design / licensing phases of **AP1000** development, which are then used and / or confirmed by calculations undertaken during cycle-specific safety evaluations. The SAC was recognised by ONR as an obvious and effective means for Westinghouse to meet SAP FA.9, but it would need to be updated to include parameters from ATWS evaluations which are part of the design basis for the UK. As a result, Action 1 was written for Westinghouse to include the MTCs used in the (Ref. 41) work into the SAC.

48. The GDA Issue action was written in 2011 not knowing that there would be a pause in the regulatory process. While Westinghouse was away from the UK, the **AP1000** detailed design and computer modelling continued to evolve as plants were constructed and near operation in the US and China. As part of the response to GDA Issue GI-AP1000-FS-02 (Ref. 6), Westinghouse has chosen to refresh its ‘standard’ plant analyses for design basis faults (ie the modelling of those faults which are considered in the same way in all **AP1000** countries) and resubmit them to ONR for inclusion in the PCSR. However, the GDA Step 4 ATWS evaluations (Ref. 41) were unique to the UK. Westinghouse stated at the start of the interactions on this action that it was confident that the differences in the **AP1000** design and computer modelling introduced between 2010 and 2015/16 would be very small on the ATWS evaluations and therefore it proposed not to update the totality of Ref. 41. It did, however, commit to reanalysing three of the more limiting ATWS events from the original report to confirm its assertions and to demonstrate that **AP1000** reactor continues to meet ATWS acceptance criteria. The results of these three calculations are reported in the main GI-AP1000-FS-03 submission to ONR (Ref. 22) and the supporting calculation note (Ref. 24).

4.1.2 Assessment

49. In Ref. 22, Westinghouse has chosen to reassess the following ATWS events using the latest versions of the LOFTRAN, ANC and VIPRE-01 codes, and assuming a January 2015 design reference point for the **AP1000** plant established in Revision 6 of Ref. 23:

- turbine trip
- loss of normal feedwater
- uncontrolled RCCA bank withdrawal

50. Westinghouse states in Ref. 22 that these were chosen because they represent a broad spectrum of conditions and plant characteristics concerning reactivity and

primary circuit pressure increases, and are therefore well suited to evaluating the impact of a change in design reference point. I am content with this reasoning and the three events selected.

51. Westinghouse's analysis methods, including those for ATWS events, were assessed in detail in GDA Step 4 (Ref. 1), including through the commissioning of independent confirmatory analysis. I have chosen not to re-examine Westinghouse's fundamental approach to ATWS modelling since it has not changed since the Step 4 assessment was undertaken. The conclusion of the previous assessment was that Westinghouse's approach met the expectations of the SAPs, including the AV series on the validity of data and models (identified as FA.17 to 24 in the version of the SAPs that existed at the time, 'rebadged' in the latest revision, Ref. 13, as AV.1 to 8).

52. Westinghouse's claim is that although there have been some changes in its approach to modelling ATWS since the original UK-specific analysis was performed circa 2010, the overall conclusions given in the PCSR on the adequacy of the **AP1000** design remain appropriate. The three sensitivity cases presented in Ref. 22 support this conclusion; while there are minor differences in temperatures and timings of key events predicted, the overall trends, results and margins to applicable acceptance criteria are all similar and acceptable.

53. It would be a significant task for both Westinghouse and ONR to 'unpick' the impact of each of the multiple minor changes that have been made to computer codes, **AP1000** models and design changes which taken together modify the ATWS predictions, and I considered this task to be of little value given that predictions remain essentially the same and I have confidence in Westinghouse's methods and processes.

54. As part of ONR's assessment of GI-AP1000-FS-02 (supported by the GRS review, Ref. 16), the differences between generations of Westinghouse analyses have been considered. The most significant changes to the standard plant design basis analyses (ie the analyses of events which are common to all **AP1000** countries and not unique to the UK) were introduced as part of an Advanced First Core Program (AFCAP) undertaken circa 2009/10. The original UK-specific ATWS evaluations reported in the PCSR were consistent with this approach. Although ATWS faults have not been considered specifically as part of the GI-AP1000-FS-02 work, the impact of the changes introduced to the modelling of the same initiating events assuming a successful reactor trip has been shown to be small.

55. In response to Action 2 of GI-AP1000-FS-02, Westinghouse has produced a UK-specific SAC (Ref. 42). Included within this (in a change to the equivalent document written for the standard plant) are limits of the following, which come from considering ATWS events within the design basis:

- MTC limits
- moderator density coefficients limits (versus coolant density)
- isothermal temperature coefficient limits
- doppler power defect limits
- differential boron worth limits

56. The expectation of GI-AP1000-FS-02 Action 2, and indeed Westinghouse's original strategy, was that values specified for these limits would come from the 2010 ATWS work (Ref. 41). However, in the course of doing this work, Westinghouse determined that two of the limits identified from Ref. 41 (the most negative MTC and the differential boron worth) could not be confirmed for all future cycles. However, the equivalent limits resulting from the three limiting cases presented in Ref. 1 could be. As a result, the SAC includes limits which are referenced to calculations performed in 2016.

57. I have no objections to this altered approach. Crucial to my assessment is that ATWS events are now firmly established as being within the UK design basis by the fact that the key limits (including the MTC specifically mentioned in the GDA Issue action) are captured within the SAC (Ref. 42). It reflects well on the clarity and formatting of Ref. 42 that I was readily able to determine from which generation of ATWS calculations the presented limits derived. Westinghouse has committed to repeating the majority of the design basis transient analyses during site licensing (including the full set of ATWS cases considered in GDA Step 4), at which time some entries in Ref. 42 could change. However, the safety case 'infrastructure' is now in place to accommodate this. I am therefore satisfied that the expectation of SAP FA.9, that design basis analysis (in this case of ATWS events) is being used to determine limits and conditions for operation, is being met.

58. The original wording of the action asked for the MTCs assumed in the ATWS analysis to be referenced from the PCSR. The link from the PCSR to Ref. 42 is a little convoluted but I am satisfied that it is there. The introduction to Chapter 9 on internally initiated faults (Ref. 38) cites Ref. 43 as its key source of technical information. Ref. 43 in turn references the SAC (Ref. 42). However, I am satisfied that the SAC is a sufficiently prominent part of the **AP1000** fault studies safety case and core design methodology for its existence and function not to be lost.

59. On this basis, I am satisfied that Westinghouse has not only addressed the specific requirements of the GDA Issue action, but has also proactively considered the continuing applicability of its original UK approach to ATWS and performed additional work to demonstrate that it remains up to date. It is my judgement that this GDA Issue action can be closed.

4.2 GI-AP1000-FS-03 Action 2

4.2.1 Background

60. Analysis of excessive increase in secondary steam flow faults is a well-established PWR fault which Westinghouse has always analysed for the **AP1000** reactor in accordance with US regulatory requirements. The result of such an event is a mismatch between reactor core power and the steam generator load demand. Cooling of the primary circuit by an excessive increase in heat removal via the secondary side can cause a positive reactivity insertion. The main phenomenon that needs to be protected against is a departure from nucleate boiling with subsequent fuel damage. During GDA Step 4, ONR assessed the discussion and results associated with these events that were provided in the European Design Control Document (Ref. 44).

61. This original GDA submission to ONR identified two variants of the event which it classified as 'Condition II' (effectively equating it to the UK definition of a frequent fault and requiring the most limiting and onerous design basis assumptions and acceptance criteria to be applied):

- an administrative violation such as excessive loading by the operator, or Plant Control System (PLS) malfunction in the steam dump control or turbine speed control
- inadvertent opening of a steam generator relief or safety valve

62. However, in the case of the first event, Westinghouse restricted its consideration to flow increases less than 10% at full power on the basis that the PLS is designed to accommodate a 10% step load increase. In the case of the second event, it limited its consideration to the opening of a single valve. ONR commented that Westinghouse had failed to adequately consider the sensitivity of its results (crucially, the margin to departure from nucleate boiling / critical heat flux) to more excessive secondary steam flows.

63. As discussed in Section 4.1, to meet the UK expectation for a demonstration of diversity of key safety functions for frequent faults, during GDA Step 4 Westinghouse did some new work on ATWS events (Ref. 41). However, again the scope of this analysis for the first event was limited to just considering flow increases up to 10% of full power. Westinghouse asserted that the inadvertent opening of a (single) relief or safety valve will not result in a reactor trip and therefore a failure to trip is not a scenario to be considered further.

64. ONR also had some observations on the scope of Westinghouse's analysis for more severe variants of the excessive increase in secondary steam flow faults (a steam system piping failure) considered in Ref. 44. Westinghouse classified a major steam line rupture as a 'Condition IV' event and minor secondary system pipe breaks as 'Condition III' events (both approximating to the UK definition of an infrequent fault). It set out to demonstrate the resilience of the **AP1000** plant by analysing the bounding major steam line rupture fault at hot zero power. However, it was the opinion of the ONR assessor, informed by the results of equivalent analyses for Sizewell B, that although hot zero power should be the limiting assumption for demonstrating a margin to critical heat flux for the largest breaks, assuming the plant to be initially at full power could be more challenging for smaller breaks.

65. As a result of these assessment observations on the Condition II, III and IV events, at the end of GDA Step 4 ONR wrote GI-AP1000-FS-03 Action 2 requiring Westinghouse to demonstrate that the **AP1000** design has adequate protection for excessive increases in secondary steam flow faults at full power assuming appropriate flow increases more severe than the 10% or single valve opening scenarios already considered. It set the additional requirement for Westinghouse to consider both events with a successful trip and events with a failure to trip (ie ATWS event) as a result of either a mechanical failure of the RCCAs to insert or a failure of the PMS to initiate a trip. If the extant design was found not to provide adequate protection, ONR anticipated that Westinghouse would need to consider design modifications, including additional flux protection. As a result, this action was one of the several in GI-AP1000-FS-03 with close links to GI-AP1000-FS-04.

66. To address this action, Westinghouse has undertaken a significant amount of work and provided a major submission to ONR. While Westinghouse was away from the UK, the need to consider a wider range of steam line breaks at full power was identified as a requirement in the US for the standard plant (ie in addition to considering the maximum break size at hot zero power). A new section was added to the standard plant design control document (but not to the European Design Control Document, Ref. 44) which included analysis of a spectrum of steam line break (0.01 m^2 (0.1 ft^2) to 0.13 m^2 (1.4 ft^2)). The top of this range corresponds to the effective throat area of the flow restrictors that are installed in the steam generator outlet nozzle. This addition to the standard plant design control document has been included in Section 9.1.6 of the updated version of the PCSR supplied to ONR in October 2016 (Ref. 38).

67. There is not a need to demonstrate diversity for frequent faults in the US, so it was still necessary for Westinghouse to provide additional submissions to address the full scope of GI-AP1000-FS-03 Action 2. This has been included as part of Ref. 22 (ie the main submission supplied by Westinghouse for GI-AP1000-FS-03).

4.2.2 Assessment

68. I am satisfied that the consideration of a range of steam line break sizes at power in Section 9.1.6 of the PCSR (Ref. 38) addresses one aspect of this GDA Issue action. The analysis demonstrates that in the event of a steam system piping failure occurring from an at-power initial condition, core protection is maintained before and immediately following reactor trip initiated on the following parameters that are monitored by the extant **AP1000** design:

- overpower ΔT
- low pressuriser pressure
- safeguards ('S') actuation signal
- low steam line pressure
- low cold leg temperature

69. The limiting case for demonstrating a margin to critical heat flux and fuel centreline melt protection is the 0.08 m^2 (0.87 ft^2) break. This is the largest break size that results in a trip on overpower ΔT. Assuming the break occurs at 0 seconds, Westinghouse's analysis predicts that the overpower ΔT set-point will be reached at 12.9 seconds, the RCCAs will start to drop at 13.9 seconds, and the maximum core heat flux will occur at 14.9 seconds. In the PCSR, these steam line break faults have been categorised as infrequent 'DB1' faults; however, Westinghouse states that it has been able to show that key acceptance criteria usually applied to frequent faults are met, and significantly that no fuel failures will occur because adequate margins to critical heat flux and fuel centreline melt are maintained.

70. I have not attempted to repeat the GDA Step 4 assessment of Westinghouse's codes and methods for analysing these faults. I am satisfied that they remain consistent with what was previously judged to be acceptable. The applicability of recent standard plant transient analyses (which the steam line break analysis of faults at power is part of) to the UK **AP1000** declared design reference point is commented on in detail as part of the assessment of GI-AP1000-FS-02 (Ref. 45). However, in brief for this assessment report, there is not a problem with applicability.

71. The PCSR only presents the results of the limiting 0.08 m^2 (0.87 ft^2) break and provides no explicit reference to lower-tier documents which provide further details on the analysis of this case and the other breaks found to be non-bounding. This approach to referencing is consistent with that seen in US licensing documents, but it is not what I would expect to see in the best examples of UK safety case documentation. However, I am content that Westinghouse's major submission for GI-AP1000-FS-02 (Ref. 43) is referenced at the start of Chapter 9 of the PCSR (Ref. 38) and this document provides a listing of all the analysis documents that support UK **AP1000** fault studies work, including these faults.

72. I am also satisfied that the revised fault schedule included in Chapter 8 of the PCSR (Ref. 39) includes the breaks both at power and with the RCCAs already inserted (events 1.21.1 and 1.21.A respectively). The frequency classification applied to the events is clearly stated, appropriate safety functions are identified, and there are clear links to Chapter 9 sections where the detailed transient analysis can be found. This is all consistent with my expectations for a fault schedule by SAP FA.8 (Ref. 13).

73. The UK-specific expectation to demonstrate diversity in the provision of key safety functions within the design basis applies just for frequent faults. In my opinion, it is reasonable to assume that the inadvertent opening of a single relief valve via the PLS is a frequent fault while a complete guillotine break of a major steam line is an infrequent fault. However, characterising events that lie between these two extremes as either frequent or infrequent is more difficult. In this context, Westinghouse's approach to ATWS events for excessive steam increase faults as set out in Ref. 22 is sensible; before launching into transient analyses, it has undertaken a review from first principles of the possible scenarios which could cause an excessive load increase event and then estimated the frequencies associated with these scenarios to determine which should be considered as frequent faults.

74. Figure 1 shows a simplified diagram of the **AP1000** secondary system that Westinghouse has reviewed to identify both pipe breaks and valve openings. It has considered both Electric Power Research Institute (EPRI) pipe rupture frequency references and similar material issued by the Health and Safety Executive (HSE) to

estimate that breaks between 0.009 m^2 (0.1 ft^2) and 0.037 m^2 (0.4 ft^2) will have failure frequencies in the 1 x 10^{-3} per year to 1 x 10^{-4} per year range. On that basis, it has chosen to consider steam line breaks up to 0.045 m^2 (0.48 ft^2) as a bounding scenario to consider as a frequent fault. This would be an asymmetric fault, with steam being lost through one of the two steam lines.

75. Westinghouse has also looked at available data for the mechanical failure of valves in the secondary side. It has concluded that the failure of a single valve is < 1 x 10^{-2} per year, and therefore the independent failure of two valves is < 1 x 10^{-4} per year. The valves are sized such that none have a flow area larger than 0.018 m^2 (0.2 ft^2) and therefore the failure of two valves in the same line is bounded by the break fault mentioned above. I am satisfied with this approach. Attributing frequencies to breaks or valve failures is not a precise science, and by considering larger breaks or multiple failures that have a calculated frequency down to 1 x 10^{-4} per year (the definition of a frequent fault being 1 x 10^{-3} per year), Westinghouse has taken reasonable steps to consider 'cliff-edge' effects (see SAP FA.7) while still eliminating the largest breaks from its ATWS evaluations.

76. Westinghouse has also considered C&I-induced failures of the Power-Operated Relief Valves (PORVs) or the turbine bypass valves (the steam generator safety valves are spring loaded). The consequences of both PORVs opening because of a PMS failure are the same as a mechanical failure. The potential for all six turbine bypass valves opening is a more complex situation. The flow capacity of each turbine bypass valve is 6.66% of the rated main steam flow at full load, resulting in an excessive load increase of up to 40% if they were to open spuriously. This would be a severe and limiting symmetric fault if it ever occurred. However, Westinghouse states in Ref. 22 that it would require a highly unlikely combination of PLS and PMS faults for the sequence to occur. I am sympathetic to this assertion but it is a complex claim to substantiate. I therefore suggested to Westinghouse during my routine interactions on this GDA Issue that it could be a simpler and stronger safety case to demonstrate the resilience of the **AP1000** design to such an event rather than trying to justify its exclusion. Westinghouse has chosen to do this.

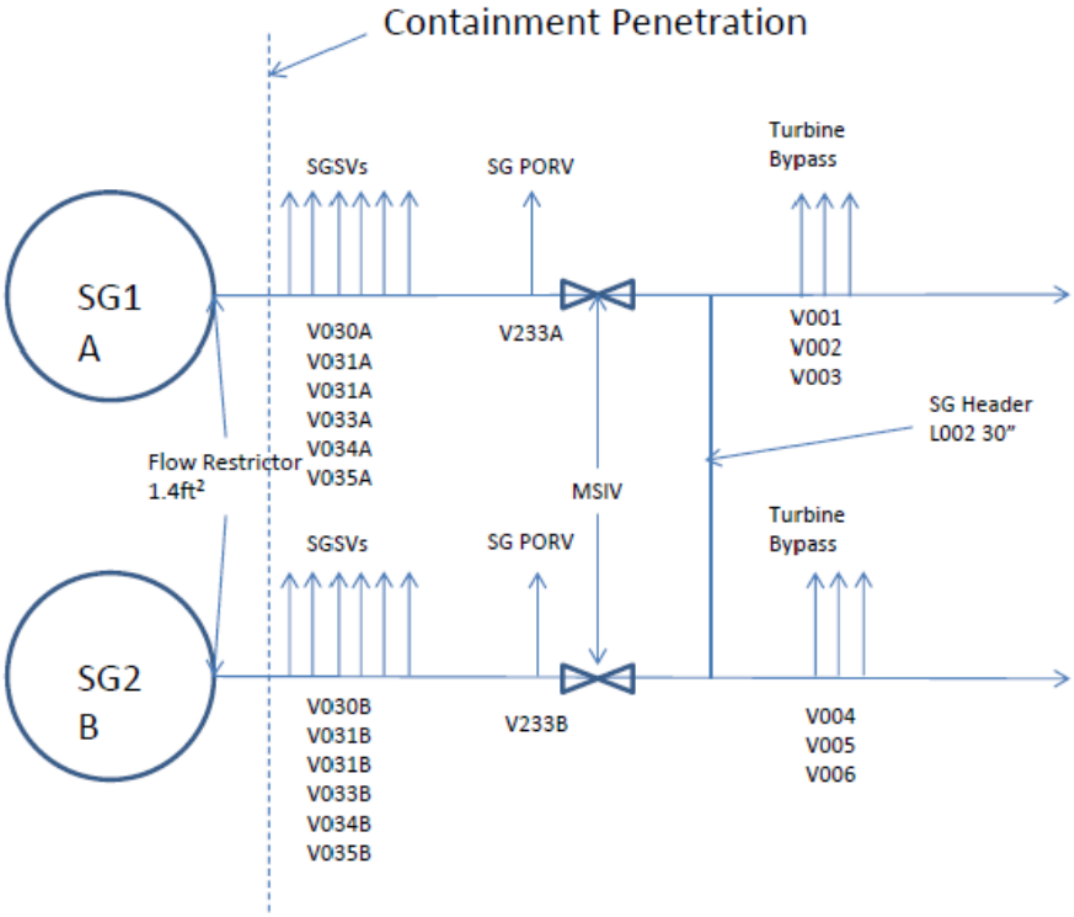

Figure 1: Simplified drawing of the **AP1000** secondary system

77. Ref. 22 summarises the transient analysis of the two limiting ATWS cases considered: the 0.045 m^2 (0.48 ft^2) rupture of a steam line that results in an asymmetric cooldown and the 40% steam load increase caused by the opening of all six turbine bypass valves that results in a symmetric cooldown. It has used the same LOFTRAN and ANC / VIPRE codes discussed in the assessment of GI-AP1000-FS-03 Action 1. For the same reasons as stated above, I am sufficiently satisfied with Westinghouse's ATWS methodology as a result of the GDA Step 4 assessment and the review of continuing appropriateness for the latest declared design reference point undertaken for GI-AP1000-FS-02 (Ref. 45) to accept the results presented in Ref. 22 at face value without a more in-depth assessment. The key assumptions made in the analysis are set out clearly in Ref. 22 while Ref. 27 provides more details on the specifics of the analyses.

78. It is important to note that Westinghouse has refined its **AP1000** LOFTRAN model for the limiting symmetric steam flow event. Consistent with other Westinghouse PWR designs, the **AP1000** plant is fitted with steam generator flow restrictors to mitigate the consequences of a major steam line break event. Westinghouse has changed the LOFTRAN steam system modelling to more appropriately model the effect that flow restrictors have on the assumed steam flow at the steam generator outlet. I am content that this is a reasonable modelling assumption to make.

79. The results of the transient analyses show that appropriate acceptance criteria for ATWS events are met, notably that margins to critical heat flux and fuel centre melt temperature limits are met. Westinghouse has also performed some sensitivity calculations without the flow restrictors. These show that at the resulting higher power levels, some acceptance criteria could start to be challenged after 30 minutes. However, these extra calculations are mainly of academic interest to show the

effectiveness of the flow restrictors and the sensitivity to hydraulic assumptions. In addition:

- Westinghouse has adopted a conservative approach for identifying excessive increase in secondary steam flow events to be considered with a failure to trip the reactor, bounding initiators with frequencies down to 1 x 10^{-4} per year.
- The inclusion of a C&I-induced common mode failure of all six turbine bypass valves combined with a failure to trip the reactor is an extreme event to consider within the design basis.
- The flow restrictors are a long-standing feature of the **AP1000** steam generators that are designed to limit the consequences of these types of events and therefore it is reasonable to credit them in the analysis.
- A large steam release event is likely to be apparent to the operators and assuming some action within 30 minutes is reasonable.

80. I am therefore satisfied that Westinghouse has undertaken the necessary work required by this GDA Issue action. More severe excessive increase in secondary steam flow events with a failure to trip the reactor than those previously considered have been analysed and Westinghouse has still been able to show that the **AP1000** plant has adequate protection without the need for further design changes. Taken together with the consideration of a range of steam line breaks at power with a reactor trip that is now included within the PCSR, it is my judgement that this GDA Issue action can be closed.

4.3 GI-AP1000-FS-03 Action 3

4.3.1 Background

81. The **AP1000** reactor has two types of control rods, both of which are grouped into various banks. The 'main' RCCA banks are grouped into three different types of banks:

- The 'SD' banks which are used only to shut down the reactor and are always kept out of the core during power operations.
- The 'AO' bank which is used to maintain the axial flux difference within a deadband about the desired target value.
- The 'M1' and 'M2' banks used for Tavg (reactivity) control. Bank M1 will typically remain out of the core but may be inserted at full power conditions while performing large load changes. Bank M2 is precluded from being inserted into the core at any power level by the plant Technical Specifications and therefore essentially acts as an additional shutdown bank.

82. The **AP1000** reactor also has four control banks of 'grey' rod control assemblies (GRCAs) which have a smaller reactivity worth relative to the RCCA banks. These banks are routinely inserted into the core during operation (some of these banks are intended to be always in the core) to maintain the average coolant temperature on its power dependent Tavg program.

83. As a well-established aspect of the **AP1000** design basis safety case, Westinghouse has always demonstrated that its plant is resilient against control misalignment faults, specifically:

- one or more dropped RCCAs/GRCAs within the same group
- a statically misaligned RCCA/ GRCA
- withdrawal of a single RCCA/ GRCAs

84. During GDA Step 4, ONR's fault studies assessment considered this aspect of the **AP1000** safety case. The most significant issue raised during the assessment was that these faults were likely to meet the criteria of a frequent fault but there was no

demonstration of diversity in protection in the safety case (Ref. 44). In response to this challenge, Westinghouse identified the dropped RCCAs event as the limiting scenario and analysed it as an ATWS scenario assuming the primary protection provided by the PMS fails. In this analysis, Westinghouse took credit for the protective function provided by the 'P-17' permissive rod withdrawal block component. This prevents the automatic rod control system from unnecessarily withdrawing control rods to compensate for the dropped RCCAs or GRCAs, thus mitigating potential power overshoots, and it works directly from signals from the ex-core flux detectors independent of the PMS

85. While not disagreeing with Westinghouse's claim that the P-17 would provide a useful and effective function, ONR observed that it was not a fully diverse capability because the ex-core detectors are also used by the PMS. Therefore, if a dropped RCCA/GRCA event occurred and the PMS failed to respond because of a failure of the ex-core detectors, the P-17 protection would also be unavailable. For this reason, Action 3 was written, requiring Westinghouse to demonstrate that the UK **AP1000** reactor has diverse protection against RCCA misalignment faults, including one or more dropped RCCAs.

86. At the time of writing the action, ONR anticipated a potential for the DAS and / or in-core detectors used by the BEACON core monitoring system to provide this diversity and ensure that margins to safety limits are ensured.

4.3.2 Assessment

87. The objective of my assessment for this action is to come to a view on Westinghouse's submissions that aim to show that there is an adequate safety case for frequent RCCA misalignment faults, assuming a failure of primary means of protection. I have not attempted to reassess the 'frontline' safety case for these faults, which was considered in GDA Step 4 (Ref. 1). However, Westinghouse's methodology for demonstrating diversity in safety provision is a variation of that originally presented in the European Design Control Document (Ref. 44) for showing the effectiveness of the primary protection. As a result, I have had to gain an additional appreciation of Westinghouse's underlying methodology to be able to assess the diversity case.

88. Of the three RCCA misalignment faults identified in Westinghouse's safety case, I have only considered the first one (one or more dropped RCCAs within the same group). Westinghouse's safety case argument for the second fault is that for even the most severe static misalignments no automatic protection (primary or diverse) is required, as the margin to the departure from nucleate boiling ratio (DNBR) safety limit is not challenged. Therefore, I have excluded it from this part of my assessment (note, in Section 4.7.2.1 I have considered in the context of GI-AP1000-FS-04 whether improvements to in-core flux monitoring could be reasonably practicable for this fault). The withdrawal of a single RCCA is classified as an infrequent fault (multiple errors would need to occur for it to happen) and therefore a demonstration of diversity is not required.

89. Westinghouse's principal submission setting out its diversity safety case arguments for dropped RCCAs is Ref. 22. It has complemented this report with several supporting references (Refs 25, 58 and 59). The updated PCSR (Ref. 38) summarises the approach and results for both the primary and diverse protection cases for these frequent RCCA misalignment faults. I have not looked again at the original safety case discussion for these faults included in the European Design Control Document (Ref. 44) that was considered during GDA Step 4. Note, the differences between generations of Westinghouse analyses have been considered as part of ONR's assessment of GI-AP1000-FS-02 (supported by the GRS review, Ref. 16).

90. Westinghouse's methodology uses:

- the LOFTRAN code to calculate the nuclear power, core heat flux, RCS temperature and pressure transients resulting from the event
- the ANC code to calculate the core response, including peak linear heat rate
- the VIPRE-01 code to calculate the DNBR

91. Consistent with earlier statements, I have not repeated the GDA Step 4 assessment of the adequacy of these computer codes and I have assumed that they are adequate for the applications they have been applied to. I have observed as I have undertaken this assessment that the initial conditions and assumptions applied to the methodology are clearly documented and described in the references identified above, consistent with SAP AV.5.

92. Westinghouse's analysis route results in a large number of cases (more than a thousand) considering a range of MTCs and dropped rod worths (the amount of negative reactivity inserted into the core by the dropped RCCAs). This methodology is designed to cover all possible combinations of RCCA drop events (single or multiple) at any point in an operating cycle, without having to identify a specific scenario or RCCA location. The results are then compared against nuclear enthalpy rise hot channel factor limits ($F_{\Delta H}$) calculated to correspond to the DBNR safety limit.

93. The same methodology is used for demonstrating the effectiveness of the primary protection (as summarised in the PCSR, Ref. 38) and for the diversity analysis for this GDA Issue action (Ref. 22). However, some notable differences in analysis assumptions are made:

- The analysis for the primary protection assumes a PMS reactor trip on low pressuriser pressure (although only a fraction of the 1,000+ cases will be severe enough to reach the reactor trip set-point). The diversity analysis takes no credit for this PMS function.
- The analysis for the primary protection assumes that the M banks are under automatic rod control (such that the control system attempts to respond to the negative reactivity insertion by withdrawing RCCA banks, with a risk of a power overshoot) and with the P-17 rod withdrawal block available to limit unnecessary power increases. The diversity analysis also assumes automatic rod control but assumes that the P-17 function has failed.
- In the primary analysis, Westinghouse has assumed a constant positive reactivity insertion rate (ie the incremental rod worth) of 11 pcm/step for the RCCA banks and 4 pcm/step for the grey GRCA banks to generate transient statepoint conditions. For the diversity analysis, a constant differential rod worth of 6 pcm/step has been assumed for both the RCCA and GRCA banks.
- The primary analysis aims to demonstrate with a high degree of confidence that there remains a margin to critical heat flux (and fuel damage) by assuming a conservative safety analysis DNBR limit and a bounding axial power shape. Westinghouse has stated that this is a very conservative DNBR limit that includes margin to provide the operators some 'headroom' for potential future changes in operation, analysis and core design. For the diversity analysis, Westinghouse has assumed a slightly less conservative DNBR limit and axial power shape relative to the primary case.
- The primary analysis uses a bounding pre-fault axial power shape (resulting from a very conservative xenon skewing assumption) when confirming the $F_{\Delta H}$ limits versus dropped rod worth, is met. In the diversity analysis, xenon skewing is restricted to a 'better estimate' [redacted] of the axial flux difference targeted by the control system (noting that this is still conservative with respect to the [redacted] specifications established by the **AP1000** technical specifications for controlling the reactor with BEACON inoperable).

94. I am content with all the changes in assumptions made in the diversity analysis. The approach for the primary analysis is rightly very conservative because it is considering a frequent fault. The likelihood for the scenario considered in the diversity analysis occurring is much lower (an RCCA drop *and* a failure of the PMS). The concept of varying the confidence level in a design basis calculation according to fault frequency is established as UK relevant good practice (see Section 5 of Ref. 60). None of the relaxations in assumptions have reduced the calculation to a truly best estimate evaluation and several conservatisms from the primary analysis remain unaltered.

95. The result of Westinghouse's analysis of the 1,000+ cases is that in all instances the revised DNBR limit was met. The most limiting heat flux results occur near Beginning of Cycle (BOC) conditions when the MTC is least negative, but even in these cases there is always a margin between the maximum transient values and the corresponding DNBR limit. As a result, Westinghouse states in Ref. 22 that the **AP1000** reactor will remain safe with respect to dropped RCCA events even if the PMS reactor trip and P-17 rod withdrawal block functions are inoperable. Therefore, no design changes such as negative rate flux trip on the DAS are needed to meet the UK's expectations for diverse protection for frequent faults. Based on Westinghouse's analysis, I agree with this conclusion.

96. Before finalising my assessment of Westinghouse's response to this action, I pursued three additional points through a regulatory query (Ref. 61). The first point I sought assurances on was whether Westinghouse's methodology needed a capability to consider asymmetric RCCA/GRCA drop faults. The definition of the fault being considered is one or more control rods *in the same group* being dropped. The non-shutdown controls rods that are inserted into the core during power operations, whether they are RCCAs or GRCAs, are grouped into radially symmetric banks of four. This ensures that when they move, their effect is distributed around the core and not localised. If in a fault condition a single RCCA/GRCA within a bank is dropped, the effect will inevitably be asymmetric (unless it is a control rod in the centre of the core) but Westinghouse's methodology allows for this by making conservative assumptions. However, if two or three control rods drop in an asymmetric pattern, it could potentially result in a greater $F_{\Delta H}$ than that assumed in Westinghouse's methodology.

97. In its response to the regulatory query (Ref. 61), Westinghouse has explained that the **AP1000** design has engineering features within the rod control system which ensure that RCCAs/GRCAs are always moved in their assigned banks. It states that there is a specific design requirement that "no single failure shall cause an asymmetric rod drop other than a single rod drop". This requirement is met by rigorous factory acceptance tests, a 'double-hold' design feature to grip the control rods, and redundant power circuits to the control rod drive mechanisms. Based on this information, I am satisfied that Westinghouse's analysis methodology is consistent with the engineering features (which include some improvements from earlier reactor designs) provided to prevent asymmetric drops involving more than one RCCA/GRCA, and therefore the conclusions reached by the diversity analysis are robust.

98. The second point I questioned Westinghouse further on was the adequacy of the prompts to the operator to take action following a fault and whether it would be reasonably practicable to increase the safety classification (and therefore reliability) of the indications. While the diversity analysis demonstrates that the DNBR safety limits are not challenged if no credit is taken for the PMS and P-17 automatic rod withdrawal block, it would be undesirable to unknowingly stay in an abnormal condition for a prolonged period of time. Assuming the PMS has failed, the operators would be reliant on the Class 3 rod position indication system for information on the status of the RCCAs/GRCAs.

99. In the response to the regulatory query (Ref. 61), Westinghouse has extended the modelling of the control rod drop fault out for several hours (the original analysis in Ref.

22 only considered the challenging first few seconds after the fault has occurred). This extended analysis shows some changes in local and peak power over time as the core adjusts to the dropped control rod and changes in xenon distribution, but no behaviour that challenges safety limits. If the operator and plant control system continued to run the plant assuming nothing was wrong, then even these tolerable variations are unlikely to occur. On this basis, Westinghouse states that it does not consider it to be reasonably practicable to increase the safety classification of the rod position indication system. I agree with this conclusion.

100. The final point I asked Westinghouse about in Ref. 61 was PCI. PCI is not discussed in the submissions for this action. As stated in Section 2.5 above, in GDA Step 4 Westinghouse produced a report setting out the limits it would apply to the **AP1000** reactor to protect against the phenomenon (for a range of faults) and the 3D FAC methodology it has developed to ensure that these limits are complied with (Ref. 62). However, the application of the methodology to frequent RCCA/GRCA misalignment faults was postponed until site licensing.

101. In its response to Ref. 61, Westinghouse reaffirmed that its methodology for the primary analysis (and by extension its diversity analysis) has not been changed for this GDA Issue closure work to consider PCI failures. However, it remains confident that it will be able to demonstrate in site licensing that the PCI criterion is met. I am content with this response. Westinghouse's approach to PCI (for GDA and beyond) was assessed and judged to be adequate during GDA Step 4. There is no expectation or reason to re-examine these conclusions as part of GI-AP1000-FS-03. As a result of the response to Ref. 61, I am now fully aware that Westinghouse's methodology for demonstrating the effectiveness of the primary protection for control rod drop events methodology has still to be updated to consider PCI effects. Although I have needed to consider this methodology to gain an understanding of the diversity analysis, it was not itself under review.

102. In conclusion, having considered Westinghouse's principal submissions, supporting references and responses to regulatory queries, I am satisfied that the **AP1000** reactor has an adequate safety case for frequent control rod misalignment faults assuming a failure of the primary protection systems. It is my opinion that Westinghouse has fully addressed the requirements of the GDA Issue action and it can be considered closed.

4.4 GI-AP1000-FS-03 Action 4

4.4.1 Background

103. As a well-established aspect of the **AP1000** design basis safety case, Westinghouse has always demonstrated the ability of the PMS to protect against uncontrolled RCCA bank withdrawal faults at power. In the European Design Control Document (Ref. 44), Westinghouse classified this event as Condition II (equating to a frequent fault in UK terminology) and showed through conservative analysis that appropriate acceptance criteria could be met. However, ONR's initial GDA Step 3 assessment found no documented consideration of RCCA bank withdrawal ATWS events in accordance with UK relevant good practice. A wide-ranging regulatory observation was raised which resulted in Westinghouse analysing a number of ATWS events, including RCCA bank withdrawal faults, during GDA Step 4 (Ref. 41).

104. While the need to demonstrate diversity for design basis frequent faults is a UK-specific expectation, internationally (notably the US) there are requirements to consider ATWS events (outside the design basis) and to take credit for defence-in-depth systems in PSA evaluations. At about the same time it set out to produce Ref. 41, Westinghouse established a requirement to modify the design of the DAS to include a reactor and turbine trip function triggered by a high hot leg temperature signal to support its standard plant ATWS analysis and PSA modelling. This resulted in

a DCP, APP-GW-GEE-1481 (Ref. 30), being drafted to introduce this functionality across all **AP1000** plants, including the UK design.

105. Westinghouse took credit for this change in its UK ATWS analysis included in Ref. 41 even though it had not been formally incorporated into the design by this stage. It was ONR's judgement that the submitted analysis showed that this design change would have a significant safety benefit for the **AP1000** design and it therefore strongly welcomed it (Ref. 1). However, given that it was not discussed or recognised in the principal safety case documents assessed during GDA Step 4, GI-AP1000-FS-03 Action 4 was written to ensure that it was implemented into the design and credited in the safety case, notably the PCSR and fault schedule.

4.4.2 Assessment

106. Towards the end of GDA Step 4, after ONR had completed its fault studies assessment and written GI-AP1000-FS-03 Action 4, Westinghouse formalised its design at a reference date of September 2010 in Revision 5 of the "AP1000 Design Reference Point for UK GDA" report (Ref. 23). APP-GW-GEE-1481 (Ref. 30) was included in this design reference point but flagged as an 'unincorporated' change.

107. Following its return to the UK regulatory process, Westinghouse supplied Revision 6 of Ref. 23 with a new design reference date of January 2015. This report stated that the design change's status had moved from 'unincorporated' to 'incorporated'. Therefore, at face value, Westinghouse had addressed the requirements of this GDA Issue action. However, I chose to investigate further what the implications were for UK **AP1000** design of Westinghouse declaring a design change incorporated. With regard to this specific change, I had a number of initial concerns for which I was looking to gain additional assurance before concluding that the requirements of the action had been met:

- DCP APP-GW-GEE-1481 was written circa 2010. It was intended to be a standard plant change (ie applied to all **AP1000** plants proposed around the world, including the UK). However, at the time Westinghouse's standard DCP template did not prompt the DCP author to consider the impact of the proposal on non-standard plant documentation, in particular the UK PCSR and fault schedule. Given that the change was incorporated while Westinghouse was not actively considering UK regulatory matters, I needed to gain confidence that all impacted UK documentation had been updated, in the absence of a formal prompt and perhaps motivation to do so. *Note, Westinghouse's DCP template has subsequently been improved to clearly identify the impact of changes in various regulatory jurisdictions.*

- During GDA Step 4, Westinghouse committed to making some significant changes to the design of the DAS on the UK **AP1000** plant through two other DCPs (Refs 46 and 47). Therefore, it was anticipated that the way in which the changes would be included within the UK DAS C&I architecture would be different from the standard plant, and new / revised documentation written to capture the broader DAS changes (unfamiliar to the original authors of APP-GW-GEE-1481) might need to be updated.

108. I have chosen not to assess the completeness with which Westinghouse has implemented APP-GW-GEE-1481 into the standard plant design. I am sufficiently satisfied with Westinghouse's normal design change process (see the parallel assessment of GI-AP1000-FS-01, which considered this aspect in more detail, Ref. 32) to take it as given that the standard plant design does include a DAS reactor and turbine trip function triggered by a high hot leg temperature signal. However, I have examined the key UK fault studies submissions for evidence that the design change has been credited.

109. Chapter 8 of the PCSR includes the fault schedule. A fault schedule was included in Revision 0 of the PCSR (Ref. 37) produced towards the end of GDA Step 4, but not formally assessed by ONR. Following its re-entry to GDA, Westinghouse has been regularly updating the fault schedule to incorporate its work for GDA Issue GI-AP1000-FS-08 (Ref. 48), any changes to the identification of faults and their protection coming from the other 50 GDA Issues (including the two GDA Issues considered in this assessment report), and any general improvements identified by Westinghouse during its update of the PCSR (GI-AP1000-CC-02, Ref. 11). To come to a view on the adequacy with which the fault schedule includes the design change, I have looked at the version of Chapter 8 supplied in October 2016 (Ref. 39). While not the final version of the fault schedule (which will be issued as part of the final PCSR when all 51 GDA Issues are closed), it is significantly changed from that included in Revision 0 of the PCSR (Ref. 37).

110. I was able to confirm that Ref. 39 does show the DAS high hot leg trip as providing diverse protection for the following events (assuming a failure to trip on the PMS):

- uncontrolled RCCA bank withdrawal at power
- uncontrolled RCCA bank withdrawal from a subcritical or low-power startup condition
- partial and complete loss of forced reactor coolant flow
- CVS malfunction that results in a decrease in the boron concentration in the reactor coolant

111. The fault schedule entries refer to relevant sections of Chapter 9 of the PCSR where analyses demonstrating the effectiveness of the claims made in the fault schedule are provided. Again, I have looked at an interim version of Chapter 9 for my assessment (Ref. 38), choosing not to look at the original submission (Ref. 37) or to wait for the final version of the PCSR to be produced. From this review, I am satisfied that the relevant sections of Chapter 9 identified by the fault schedule do indeed credit the existence of the DAS high hot leg trip. The source of the ATWS analyses summarised in the Chapter 9 sections crediting the DAS high hot leg trip is Ref. 41(which was the work that originally ONR assessed during GDA Step 4 and which prompted this GDA Issue action to implement the change).

112. As a result of this review, I am satisfied that the impacted fault studies documentation has been adequately updated to reflect the change.

113. A significant UK-specific C&I document that supports the PCSR and which is impacted by this design change is the “United Kingdom AP1000 Basis for the Safety Case of the 7300 Series Based Diverse Actuation System” (Ref. 49). However, the need to update this document was not identified in the standard plant DCP (Ref. 30). Revision 0 of Ref. 49 was produced in 2010 contemporaneously with the drafting of APP-GW-GEE-1481 and the UK ATWS analysis (Ref. 41). By reviewing this original revision, I have been able to establish that the DAS high hot leg trip was included back in 2010.

114. Since Westinghouse has returned to the GDA process, it has been working to address the two significant DCPs (Refs 46 and 47) which change the DAS’s voting logic and platform, and the two DAS-related GDA Issues (Refs 17 and 18). In July 2016, Revision 1 of the Basis for the Safety Case report was provided to ONR, reflecting the work to date (Ref. 49). A review of this version of the report shows some significant changes to the text, including those aspects related to the high hot leg trip. However, the requirements established by the ATWS work and the fault schedule remain unaltered, and the fact that this aspect is demonstrably subject to ongoing evaluation gives me confidence that it is a well-established feature of the design.

115. The requirement established by the ATWS work and the fault schedule is the need for an automatic Class 2 trip of the reactor and turbine as a diverse back-up to the Class 1

PMS for frequent faults. Westinghouse has chosen to provide this functionality by the DAS. There are established expectations for the engineering requirements of the Class 2 C&I system. The stated objectives of the Basis for the Safety Case report for the DAS (Ref. 49) are to demonstrate:

- a safety lifecycle based on IEC 61513 (Ref. 50) for a Class 2 system with a reliability claim of 1.0 $x10^{-2}$ probability of failure on demand (pfd);
- conformance to applicable SAPs for a Class 2 system;
- the DAS design reduces risks to As Low As Reasonably Practicable (ALARP); and
- the production excellence of the DAS is commensurate for a Class 2 system with a reliability claim of 1.0 $x10^{-2}$ pfd.

116. I am satisfied that the high hot leg trip functionality is included with the DAS scope being considered in Ref. 49. On the basis that my C&I colleagues will need to satisfy themselves as part of their assessments of the DAS that this key report meets its stated objectives (see Refs 17 and 18), then I am content to assume that the design details proposed for the UK implementation of the APP-GW-GEE-1481 (Ref. 30) are adequate (or will be modified as part of the work to close the C&I GDA Issues) for a Class 2 system without undertaking a detailed assessment myself.

117. On that basis, I am satisfied that Westinghouse has adequately implemented the diverse hot leg trip function, crediting it appropriately into the relevant UK safety case documentation and including the functionality in the wider C&I-related work to modify the DAS to meet UK expectations. I recommend that the GDA Issue action can be closed.

4.5 GI-AP1000-FS-03 Action 5

4.5.1 Background

118. In its original submission to ONR (Ref. 44), Westinghouse demonstrated that it had considered as a design basis event a complete loss of reactor coolant flow as a result of the simultaneous coasting down of all four Reactor Coolant Pumps (RCPs). It summarised transient analyses which demonstrated that the PMS can trip the reactor quickly enough to avoid departure from nucleate boiling, in a race between the speed of the RCPs coasting down and the speed of the protection system and time for the RCCAs to insert.

119. Westinghouse extended its consideration of this event during the GDA Steps 3 and 4. Acknowledging that the initiating frequency is high enough for it to be considered frequent within the traditional UK approach to design basis analysis, Westinghouse analysed an ATWS version of this event to demonstrate diversity in the provision of the reactivity safety function (Ref. 41).

120. ONR assessed both the original submission (consistent with the standard plant analyses) and the UK-specific ATWS evaluations during GDA Step 4. Despite being content that the appropriate events had been identified and analysed, ONR was not satisfied that the assumptions made in the transient analysis were limiting and therefore consistent with the expectations for design basis analysis set out in SAP FA.7.

121. A potential reason for a complete loss of reactor coolant flow is a loss of electrical supplies to the RCPs. Westinghouse's analysis, both for the 'normal' event (ie with a successful reactor trip) and the ATWS case, assumed that the plant would be operating at nominal full power conditions prior to the event. However, ONR observed that it was likely that a loss of electrical supplies could have been preceded by grid frequency perturbations. The primary impact of a grid frequency perturbation would be

on equipment that runs on Alternating Current (AC) power supplied from the grid, notably the RCPs and Main Feedwater Pumps (MFWPs). If the reactor and turbine control systems attempt to compensate for variations on primary and secondary flows, there is a potential to perturb both the initial (total) power and the power distribution in the core (compared with that assumed in Westinghouse's analysis) prior to a trip parameter set-point being reached.

122. It was also observed that Sizewell B is provided with an RCP underspeed trip on both its primary protection system and its diverse secondary protection system. **AP1000** design is provided with an RCP underspeed trip on the PMS only. As a result, Action 5 was written requiring Westinghouse to demonstrate the adequacy of the **AP1000**'s protection against a complete loss of forced flow faults as a result of perturbations in grid frequency for both reactor trip cases and where the RCCAs fail to insert due to a mechanical or PMS failure.

4.5.2 Assessment

123. Westinghouse's response to this GDA Issue action has been principally provided in Ref. 22. This has been the main document I have considered to come to a judgement on whether this action can be closed. I have also considered the supporting calculation note (Ref. 28) and I have held multiple discussions with Westinghouse on its strategy for addressing this action.

124. SAP FA.6 sets an expectation that design basis analysis considers the most onerous initial operating state within the inherent capacity of the facility permitted by operating rules. The UK grid code (Ref. 51) establishes requirements for electricity generating units, including the magnitude of frequency variations that the plant must survive without tripping.[1] It therefore follows that unless a future licensee applies for a specific derogation, an **AP1000** unit connected to the grid must have operating rules that are consistent with grid code requirements.

125. Westinghouse states in Ref. 22 that it has reviewed the applicable section of the grid code (CC.6.1.3) and identified the requirements set out in Table 1.

126. After consultation with specialist electrical engineering colleagues, I am satisfied that Westinghouse has identified the appropriate grid code requirements and I am content that these provide a sensible basis for identifying perturbed conditions to consider in revised transient analyses.[2] Westinghouse has chosen to conservatively disregard the 'survival times' set out in Table 1 and to only consider the extremes (47 Hz to 52 Hz), with 50 Hz as the nominal grid frequency. Again, I am satisfied that this is a sensible analysis choice to make.

[1] In the event that the grid is suffering stability problems due to generation or load problems / variations elsewhere, the National Grid does not want other large generating units (such as an **AP1000**) tripping unless absolutely necessary, as this would just further exacerbate the problems.
[2] In Ref. 22, Westinghouse has identified Issue 5 Revision 15 of the grid code (February 2016). At the time of writing this assessment report, the most up-to-date public version was Issue 5 Revision 17 (June 2016). However, the grid frequency variation requirements were unchanged.

Table 1: Grid frequency variations identified by Westinghouse from the UK grid code

CC.6.1.3: The System Frequency could rise to 52Hz or fall to 47Hz in exceptional circumstances. Design of User's Plant and Apparatus and OTSDUW [Offshore Transmission System Development User Works] Plant and Apparatus must enable operation of that Plant and Apparatus within that range in accordance with the following:	
Frequency Range	***Requirement***
51.5Hz - 52Hz	*Operation for a period of at least 15 minutes is required each time the Frequency is above 51.5Hz.*
51Hz - 51.5Hz	*Operation for a period of at least 90 minutes is required each time the Frequency is above 51Hz.*
49.0Hz - 51Hz	*Continuous operation is required.*
47.5Hz - 49.0Hz	*Operation for a period of at least 90 minutes is required each time the Frequency is below 49.0Hz.*
47Hz - 47.5Hz	*Operation for a period of at least 20 seconds is required each time the Frequency is below 47.5Hz.*

127. The RCPs on the **AP1000** reactor are provided with Variable Frequency Drives (VFDs) that regulate the frequency from the grid to the RCP motor. The VFDs are used to start and stop the pumps, and in the case of the UK **AP1000** design continue to operate once the reactor has reached full power because the grid is 50 Hz and the RCP motors are designed to operate at 60 Hz (in other countries with 60 Hz grids, notably the US, the VFDs are not needed once the reactor reaches full power). As a result, should the grid frequency vary, the VFDs could accommodate the perturbations and the RCPs would be minimally affected. However, Westinghouse has rightly recognised that the VFDs are not Class 1 or 2 safety systems and therefore they cannot be credited to perform their function in a design basis event unless their correct performance makes the transient worse (in accordance with SAP FA.6).

128. The MFWPs are not connected to VFDs or any other frequency-regulating device and therefore their speed would inevitably change with a perturbation in grid frequency.

129. In Ref. 22 and the supporting document Ref. 28, Westinghouse has analysed a range of cases considering different perturbation cases and responses of affected systems, and compared the results with its latest 'analysis of record case' (ie, the analysis of the same event considered by ONR in the GDA Step 4 assessment but updated to reflect the latest design reference point and using the latest versions of Westinghouse's computer codes). I consider the list of cases identified by Westinghouse to be thorough and systematic, considering a range of behaviours of the VFDs and MFWPs, different RCCA responses, and both BOC and End of Cycle (EOC) reactivity conditions.

130. Given that Westinghouse's LOFTRAN and VIPRE methodologies for assessing loss of reactor coolant flow faults is essentially the same as that assessed by ONR during GDA Step 4 (judged at that time to be satisfactory), as part of this assessment I have chosen not to look at it again. The impact of moving to a design reference point and applicability of Westinghouse's latest analysis to it is assessed outside this report as part of GI-AP1000-FS-02 (Ref. 6). While it was undertaking this analysis, Westinghouse itself discovered a long-standing but small non-conservatism in one of the LOFTRAN code input parameters. This was brought to my attention during the course of my interactions with Westinghouse and its normal in-house corrective action procedures for managing such an occurrence were explained to me. I was satisfied

with the process and that it was demonstrably followed, that the implications for this analysis of the error are small, that the wider implications for Westinghouse's design basis analysis are small, and that ONR's original GDA Step 4 conclusions are unaffected.

131. The most limiting case (in terms of margin to DNBR limit) identified by Westinghouse assumed that the reactor flow was at 100% (ie the VFDs operated as designed) and the MFWP flow at 104% (in response to a +2 Hz frequency change from the nominal 50 Hz), with the RCCAs under automatic control and assuming BOC reactivity feedback conditions. However, the safety analysis limit on minimum DNBR limit was shown to be met and a comparison presented by Westinghouse in Ref. 22 of the power-to-flow ratio variation with time showed no significant difference between this perturbed case and its 'standard' case assuming nominal pre-fault at-power conditions.

132. On the basis of this new presentation of a range of sensitivity cases, I am satisfied that Westinghouse has addressed the first aspect of this GDA Issue action to show that grid frequency perturbations associated with the conditions leading up to a loss of reactor coolant flow fault do not challenge its stated safety case claims for events where the PMS successfully trips the reactor.

133. In Ref. 22, Westinghouse has argued that it does not need to undertake additional sensitivity cases to the ATWS analyses of loss of reactor coolant flow faults to address the second aspect of the GDA Issue action. This is on the basis that the 'tripped' cases discussed above show little sensitivity to grid frequency variations and changes in RCP / MFWP flow within the ranges considered (compared with Westinghouse's 'standard' analysis at nominal conditions). As a result, ATWS analysis of the loss of reactor coolant flow faults would be expected to show a similar insensitivity. Ref. 22 does say that Westinghouse expects to consider grid frequency perturbation ATWS cases when it repeats large swathes of its **AP1000** transient analysis during site licensing activities.

134. For the purposes of closing out this GDA action, I am satisfied by these arguments. Westinghouse's original GDA Step 4 ATWS analysis for loss of reactor coolant flow faults showed that acceptable results could be achieved without further modifications, for example a low RCP trip on the DAS similar to that included on Sizewell B. Westinghouse's power-to-flow ratio plots suggest that frequency variations within the ranges established by the grid code should not alter the conclusions reached during GDA Step 4. It is therefore my judgement that this second aspect of the GDA Issue action can be considered closed and no design change is needed for either the 'tripped' or the ATWS case.

135. For completeness, I have examined how the revised PCSR (Ref. 38) incorporates the work for this GDA Issue action. I have been able to confirm that the new analysis considering frequency variations has been both discussed and referenced in Chapter 9. It is my view that some minor changes to the text could provide additional clarity. However, given that Ref. 22 is clearly referenced, I am satisfied that the potential impact of grid frequency perturbations has been adequately captured within the PCSR. All aspects of this GDA Issue action should be considered addressed.

4.6 GI-AP1000-FS-03 Action 6 and Action 7

4.6.1 Background

136. ONR expects design basis safety cases to consider all operating modes, including shutdown modes (SAPs ERC.1 and FA.6). The expectation that diversity will be demonstrated for frequent faults therefore applies equally to shutdown modes as it does for faults occurring while the reactor is at power.

137. RCCAs are not the only means of controlling reactivity in the **AP1000** core. The principal way of inserting positive reactivity into the core is by the addition of unborated water to the RCS from the Demineralised Water Transfer and Storage System (DWS) through the reactor makeup portion of the CVS. The potential for an inadvertent boron dilution event has been considered by the **AP1000** designers, with thought given to how the operations are controlled, how the size of any dilution can be minimised, and what flux protection is needed on the PMS to isolate the source of the dilution. Westinghouse's approach to these 'homogenous' boron dilution faults is described in the European Design Control Document (Ref. 44) and was assessed by ONR during GDA Step 4.

138. The CVS and DWS are not Class 1 systems, and therefore Westinghouse has consistently considered homogenous boron dilution faults as Condition II events or frequent faults. In response to regulatory observations from ONR in GDA Step 4, Westinghouse set out to demonstrate how the **AP1000** design has diverse protection for these faults, should they occur either while the reactor was at power or during shutdown (Ref. 44 did not provide this information). For homogenous boron dilution faults at power, Westinghouse argued that the reactivity insertion consequences are bounded by an uncontrolled RCCA bank withdrawal fault at power with protection provided by the high hot leg temperature trip on the DAS. ONR accepted this argument but it was not satisfied that any reliable diverse protection had been identified for faults occurring during shutdown. As a result, GI-AP1000-FS-03 Action 7 was written requiring Westinghouse to provide a demonstration that diverse protection existed, or propose a reasonably practicable design change to close any shortfalls against expectations.

139. One of the reasons the CVS is used after a routine reactor shutdown is to manage xenon decay. Xenon is one of a number of different isotopes produced by the fission of ^{235}U. Xenon is notable (specifically ^{135}Xe) because it has a large neutron cross-section such that it operates as a reactivity poison. In steady state power operation, the rates that xenon is created and removed are in equilibrium. Immediately following a reactor trip (which stops fission of ^{235}U), xenon continues to be generated from the beta decay of ^{135}I, causing an initial increase in the shutdown margin. However, over a period of hours, the xenon starts to decay away. The CVS gives the operators the ability to manage the changing shutdown margin following a reactor shutdown, potentially facilitating an early return to power. ONR's GDA Step 4 assessment (Ref. 1) raised concerns that only a modest reliability could be placed on the CVS and the operators controlling it, such that a problem occurring during xenon management operations should be considered a frequent fault with the potential to cause an unplanned increase in reactivity.

140. While there are diverse sources of borated water available (the CMTs, the accumulators and the In-containment Refuelling Water Storage Tank (IRWST)) to protect against these faults, Westinghouse had assumed that they would be initiated by operator action. This appeared to show a lack of diversity in the means to initiate boron injection, and also placed a high reliability claim on the operator. As a result, GI-AP1000-FS-03 Action 6 was written requiring Westinghouse to consider changes to the CVS and the automatic initiation of boron injection for such events, or to provide analysis to show that the consequences of the operator failing to ensure an adequate shutdown margin with the CVS are acceptable.

141. Westinghouse has addressed Action 7 principally through Ref. 22. However, this report's starting point is based on the outcome of parallel work for GI-AP1000-FS-03 Action 6 in Ref. 33 and GI-AP1000-FS-04 in Ref. 35. The conclusion of GI-AP1000-FS-04 is that there is a gap in the provision of flux protection for shutdown modes that is diverse from the PMS, and a design change is needed to meet UK expectations, including those set out in GDA Issue GI-AP1000-FS-03 Actions 6 and 7. The proposal

made in APP-GW-GEE-5251 (Ref. 36) is to add to the design of the DAS a function to actuate CMTs and isolate CVS dilution sources via a new sensor connection using the intermediate range flux detectors.

142. In practice, my assessment of all these related GDA Issues and actions was undertaken together. However, for the purposes of reporting action closure, I have restricted the scope of what I discuss in Section 4.6 to Westinghouse's submissions for Actions 6 and 7 (Refs 22 and 33) which take credit for the proposed design change. I will discuss in Section 4.7 my views on how Westinghouse arrived at the conclusion that this is the only change in flux protection that is needed (Ref. 35).

4.6.2 Assessment of Action 6

143. As stated above, Westinghouse has provided Ref. 33 as its principal submission for Action 6. I found Ref. 33 to be a systematic and thorough report with appropriate scope and objectives to address the GDA Issue action. It does the following:

- It summarises ONR's original GDA Issue action.
- It provides an overview of the major systems that are available on the **AP1000** reactor to borate the RCS.
- It summarises the definitions of the different operating modes identified for the **AP1000** reactor that should be considered normal and routine (Mode 1 – power operation, Mode 2 – startup, Mode 3 – hot standby, Mode 4 – safe shutdown, Mode 5 – cold shutdown, and Mode 6 – refuelling).
- It discusses how an adequate shutdown margin is calculated and ensured during normal operations.
- It identifies two fault cases for consideration associated with a failure of the CVS or the operator during operations to actively manage xenon poisoning.
- For the first case, it argues that the proposed modification to the DAS will ensure that there is sufficient diversity in delivering the reactivity control function to meet ONR expectations.
- For the second case, it states that the proposed modification cannot be credited and then goes on to argue why Westinghouse still believes the extant design is acceptable.
- As part of an ALARP assessment, it summarises international relevant good practice, guidance and operational experience, ahead of considering the practicability of further design changes.
- It concludes that the only design change necessary to address the GDA Issue action is the implementation of the DAS intermediate range flux function identified by the work on GI-AP1000-FS-04.

144. A notable point Westinghouse makes is that although xenon transients will occur after any reactor trip or shutdown (ie unplanned in response to a problem, or routine as part of normal operations, respectively), shutdown margin challenges will only be an issue for normal plant shutdowns or minor non-Loss of Coolant Accident (LOCA) events where the CMTs have not automatically actuated. Westinghouse confirmed in its response to regulatory query RQ-AP1000-1660 (Ref. 52) that the **AP1000** design places no safety case requirement on the CVS to inject boron for design basis faults which already credit boron being injected from the CMTs, the accumulators, and / or the IRWST in addition to RCCA insertion as protective measures (the resulting boron concentration will satisfy shutdown margin requirements for any subsequent xenon decay and RCS cooldown to cold shutdown).

145. In Ref. 33, Westinghouse does recognise that there was a gap in its safety case where the reactor has entered Mode 3 (hot standby) after a spurious reactor trip, a minor non-LOCA transient or a normal shutdown where the Class 1 safety systems have not actuated. Consideration of the two newly identified fault cases is designed to fill this gap:

- Case 1: The reactor has undergone a spurious reactor trip or shutdown, and no Class 1 safety systems have been challenged. The reactor is maintained in Mode 3 with the reactor trip breakers open (ie the RCCAs are inserted and cannot be withdrawn). The operators decide to compensate for changes in reactivity due to xenon by using the CVS. When the xenon has reached either its peak concentration (approximately 8 hours after shutdown) or returned to equilibrium concentrations (approximately 26 hours after shutdown), the CVS fails.
- Case 2: This is the same as Case 1 except that the failure occurs just after the reactor trip breakers have been closed in preparation for returning the reactor to critical.

146. Westinghouse states that the 'window of vulnerability' when CVS failure scenarios similar to Case 1 could occur (but bounded by it) is the majority of an outage. It has categorised a CVS failure in Mode 3 as a frequent fault (an initiating event frequency greater than $1x10^{-3}$ per year) and therefore recognised that it needs to demonstrate that two diverse means exist to protect against the consequences of the resulting power transient.

147. Westinghouse argues that the second case is more unlikely to occur and a number of specific events need to occur in a shorter period of time. In addition to the original trip or shutdown occurring without the CMTs actuating, the operators must have been able to quickly establish and address the reason for the trip (presumably trivial) at the same time as attempting to follow a xenon transient with the CVS (something that could not be done late on in the core's cycle when the boron levels in the RCS are dilute). The case then assumes that the CVS fails in the short period of time after the RCCA breakers have closed in preparation for restarting the reactor but before it has been made critical. On that basis, Westinghouse states that Case 2 should be considered an infrequent fault for which a single means of protecting against the consequences is required.

148. I am satisfied with the logic set out by Westinghouse in Ref. 33 for identifying these two cases. I judge it to be consistent with SAP FA.5 and it provides an appropriate and complete basis for addressing the requirements of the GDA Issue action.

149. For both cases, the protection against the event would be provided by the PMS. On a high source range signal, the PMS will block the source of unborated water to the CVS makeup pumps with redundant, Class 1 valves. The signal will also re-align the makeup pump suction to the boric acid tank. However, in Mode 3 the signal does not actuate the CMTs (the source range PMS function was originally provided for boron dilution faults for which the CMTs were not claimed) and as the RCCAs are already inserted, there is no reactor trip function provided. Audible alarms would be initiated indicating a need to add boron to the RCS.

150. To demonstrate diversity in reactivity control for Case 1, Westinghouse has stated that the operators could effectively achieve the necessary outcomes by responding to PMS alarms by opening the Automatic Depressurisation System (ADS) to reduce the RCS pressure to allow borated water injection from the accumulators. Independent of this, the design change proposed for the DAS (Refs 35 and 36) would also protect against the consequences of the fault by actuating the CMTs and isolating CVS dilution sources prompted by a high measurement on the intermediate range flux detectors.

151. I am satisfied that through these claims the requirements of GDA Issue Action 6 have been met for Case 1, assuming the credited DAS design change is implemented (see Section 4.7). The identified primary protection means (PMS and manual ADS actuation) is a safety case assumption rather than a realistic expectation of how the operators would respond; in a real event, the operators would respond to the alarms by manually actuating the CMT. However, the ability to respond in the stated way with the

ADS is available. I am not concerned by the reliance on the operator given the timescales available to respond to what is a slow-developing transient and because the manual actions are now backed up by the automatic response of the DAS.

152. By design, Westinghouse has made the DAS intermediate range flux functionality unavailable when the RCCA breakers are closed (it would not be possible to return the reactor to power at the end of an outage if the CMTs automatically injected every time the flux exceeded the specified set-point). As a result, the DAS cannot be credited to protect against Case 2. Westinghouse argues that this is acceptable because of the following:

- Protection is still available by source range indications on the PMS which would prompt manual boration of the RCS via the CMTs or, if needed, ADS actuation.
- It is most likely that the reactor would not go critical because there would be more shutdown margin than the minimum required by the Technical Specifications. If there was a stuck RCCA (an assumption made in the shutdown margin calculations), the operators would not attempt to return to power.
- There is a lot of time (several hours) for the manual response to PMS alarms sounding if the initial shutdown margin was not sufficient to prevent the reactor from going critical.
- If the reactor did go critical and the operators did nothing for circa 24 hours and the steam generator level was maintained by automatic feedwater flow, then the power could rise to 40%. However, Westinghouse dismisses this behaviour by the operators as incredible.
- If the steam generator water level was not maintained, then a low steam generator wide range level signal on the DAS would generate a reactor trip (ineffective if the RCCAs are already inserted) and actuate the CMTs (which would be effective).

153. I am satisfied with these arguments for Case 2 and for it to be considered an infrequent fault for which only one method of protection is formally claimed in the design basis safety case. I also judge that method of protection to be adequate, despite the lack of automation, because of the reasons set out by Westinghouse. Therefore, it is my judgement that the requirements of GDA Issue Action 6 have been met for Case 2.

154. Admirably, Ref. 33 goes further and discusses whether it would be reasonably practicable to increase the minimum shutdown margin limit included in the Technical Specifications or to make the CVS Class 1 (i.e. single failure tolerant and automatically initiated). Westinghouse concludes that both of these changes would be grossly disproportionate and I agree with this conclusion given the adequacy of its arguments for Cases 1 and 2 just assuming the extant design (with the addition of the automatic DAS initiation of the CMTs).

155. In summary, through a combination of existing design features, crediting the proposed design change to the DAS, arguments on the frequency of some events (Case 2), and discussing what operator behaviours and actions are credible, I am satisfied that Westinghouse has addressed the requirements of GDA Issue Action 6 and it can be considered closed.

4.6.3 Assessment of Action 7

156. In its response to Action 7 set out in Ref. 22, Westinghouse has accepted the gap against UK expectations originally raised by ONR in GDA Step 4 that if there was failure of the PMS (or its source range flux protection), the original **AP1000** design could not easily be shown to have additional diverse protection for a frequent homogenous boron dilution event caused by the CVS or DWS. Ref. 22 takes as its

starting point that the proposed design change to DAS (to include CMT actuation and dilution source isolation) will be included in the UK **AP1000** design and then sets out to determine adequate set-points for this new function which will ensure that appropriate safety criteria are met. The objectives of the relevant section of Ref. 22 are therefore fully consistent with my expectations for frequent design basis faults, as set out in SAPs FA.6 to FA.9.

157. The most significant information that Ref. 22 summarises in response to Action 7 is the analysis to determine appropriate set-points for the new DAS function. A typical design basis criterion for reactivity faults during shutdown would be to show that there is no return to criticality (SAP ECR.1). Indeed, Westinghouse asserts that this criterion is achieved by the PMS-initiated primary protection measures against a homogenous boron dilution event. However, for demonstration of the adequacy of the diverse protection, Westinghouse has relaxed this criterion by setting a new requirement of avoiding adding heat to the RCS. I am content with this because of the following:

- Recriticality will only occur after the failure of design features of the CVS and DWS, and the failure of the Class 1 PMS-actuated dilution isolation protection.
- Nuclear power plant reactor cores are by their nature designed to go critical. Although it would represent a loss of the control, there would not be any direct safety consequences to the workers or the public if the event is stopped before heat is generated.

158. For the purposes of its analysis, Westinghouse has normalised the flux seen by intermediate range ex-core flux detectors at hot full power to be 1.0 Fraction of Normal (FON). It presents analysis (for a number of different plant modes and equipment availability states) which shows that a set-point of [redacted] FON on the intermediate range ex-core flux detectors is sufficient for the DAS / CMTs to protect against the consequences of the dilution event, before the point heat starts to be added to the RCS (assumed to be at [redacted] FON).

159. Westinghouse summarises the computer codes and methodologies that it has used in its analysis. Westinghouse has made extensive use of the ANC code for this work. As with all the actions addressed in this assessment report, I have not undertaken a detailed assessment of the computer codes utilised as these were considered during GDA Step 4. The ANC code was assessed by ONR's fuel and core Step 4 report (Ref. 53) and judged to be a suitable tool for modelling core behaviour. This conclusion, allied with my general confidence in Westinghouse's general control, management, validation and application of computer codes in the fault studies topic area, gives me sufficient confidence in its methods to take the analysis results presented in Ref. 22 at face value and accept them as being suitable for decision-making. I also take assurance from the fact that Westinghouse's presented calculations are following methodologies set out in 'topical' reports which have been submitted to the US regulator (United States Nuclear Regulatory Commission, US NRC) for regulatory approval.[3]

160. I am satisfied with the range of sequences considered by Westinghouse (SAP FA.6) and Ref. 22 is very clear in identifying, for example, the operating mode involved, the number of RCP or Normal Residual Heat Removal System (RNS) pumps running, the RCS water volume vulnerable to dilution, and the dilution flow rates assumed.

161. The analysis shows that it would take over two hours (in the most limiting case considered, much longer in several other scenarios considered) for an inadvertent homogeneous boron dilution fault to take an initially subcritical core to a critical state.

[3] In the response to regulatory query RQ-AP1000-1705 (Ref. 54), Westinghouse has summarised the US regulatory approval status of its codes and methods, and explained their applicability to the UK-specific analyses.

Taking no credit for any operator response to Class 1 PMS and other prompts during this time, the analysis goes on to predict that it would take several minutes (93 seconds in the most limiting and conservatively modelled Cycle 1 case) for the flux seen by the intermediate range sensors to go from [redacted] FON to [redacted] FON.[4]

162. Westinghouse states that a conservative time for the CMT injection to be initiated after the DAS intermediate range flux detector set-point has been reached is about 70 seconds. CMT injection would not be instantaneous, but over a period of a few seconds the rate of increase in flux will slow, ahead of rapid power decrease.

163. In the most limiting analysis case Westinghouse has considered, there is not much margin between the time it takes the CMT injection to be initiated and be effective, and the point at which heat would start to be generated. However, I acknowledge the conservatism Westinghouse has included in the analysis and recognise the uniqueness of a Cycle 1 startup scenario. More realistic calculations considering typical reload cycles would show significantly more margin. Westinghouse actually recommends that the nominal set-point is in practice set to [redacted] FON, adding further confidence to its claim that the proposed design change to the DAS will be effective in preventing nuclear heat-up following a boron dilution event. On the basis of the analysis and discussion presented in Ref. 22, I am content with this proposal for the set-point and the conclusion that it will be effective.

164. Looking more broadly at the original requirements of Action 7, I am satisfied that it has been addressed. I have been able to confirm that both the fault schedule and fault analysis discussions in the relevant sections of the PCSR have been updated to reflect the work done for the GDA Issue action (Refs 37 and 38). I will comment further on the details of the design change to the DAS and the adequacy of its implementation into the safety case in Section 4.7.

4.7 GI-AP1000-FS-04

4.7.1 Background

165. As was stated in Section 1.2 of this assessment report, the two actions of GI-AP1000-FS-04 are closely related to the requirements of the actions of GI-AP1000-FS-03 and arose from the same concerns during GDA Step 4 about the need to demonstrate diversity for frequent **AP1000** design basis faults. The difference between the two GDA Issues is probably best characterised as alternative perspectives on the same issue. GI-AP1000-FS-03 took a fault-by-fault view of the need to demonstrate diversity for frequent faults. GI-AP1000-FS-04 sought consideration of potential improvements to the instrumentation and protection systems.

166. GI-AP1000-FS-04 Action 1 specifically asked Westinghouse to examine the feasibility of enhancing the flux protection in the **AP1000** design to provide automatic and diverse protection against frequent adverse power distribution faults. GI-AP1000-FS-04 Action 2 asked Westinghouse to demonstrate that diverse protection is provided against frequent reactivity and power distribution faults. Both actions anticipated that a modification or enhancement to the in-core detectors used by the BEACON core monitoring system in normal operation could have a role in addressing ONR's expectations.

[4] The limiting case is at the beginning of Cycle 1 where the only neutron sources in the 'clean' core are from the installed primary source rods. The sequence assumed that the operators were in the process of taking the reactor critical for the first time and paused with all the shutdown RCCA banks withdrawn. An undetected boron dilution event is assumed to start from this position. Westinghouse looked at other cases assuming a typical reload cycle design and the event occurring at the time in the cycle with the peak core reactivity. All showed a greater time to reach criticality and then to go from 10^{-6} FON to 10^{-2} FON than the limiting case.

167. As with all GDA Issues, the wording allowed Westinghouse to complete the actions by alternative means if it could be agreed with the regulator. Westinghouse sought approval to consolidate the response to the two actions into one, which itself would be closely linked to the work on GI-AP1000-FS-03. I was content with this, and indeed it is the approach I have adopted in this assessment report.

4.7.2 Assessment

168. Complementing and building upon Ref. 22 (the key submission for GI-AP1000-FS-03), Westinghouse submitted Ref. 35 as the main submission to address GI-AP1000-FS-04. My assessment of this report is set out in Section 4.7.2.1.

169. Westinghouse's conclusion for GI-AP1000-FS-03 is that a design change is needed to the DAS. My views on the need for identified functionality and whether additional modifications are required are also discussed in Section 4.7.2.1. My assessment of the technical details of how the functionality will be delivered and the adequacy of Westinghouse's processes for taking the modification forward is summarised in Section 4.7.2.2.

4.7.2.1 Adequacy of the Main Submission

170. Ref. 35 takes a twin-track approach to addressing GI-AP1000-FS-04. After summarising the functionality of the extant PMS and DAS protection systems, the report considers in parallel the following:

- The primary and diverse protection available for each increase in heat removal, reactivity and power distribution anomaly design basis event in the PCSR, and whether there is a gap in provision when compared with the UK expectations for frequent faults. Where appropriate, it takes credit for the latest analysis undertaken for GI-AP1000-FS-03.
- Independent of whether an individual fault has a shortfall against UK expectations, what technological solutions have the potential to provide diverse flux protection and for which scenarios they would be effective.

171. Westinghouse made its decision on which of the options, if any, would be ALARP to be included in the **AP1000** design informed by both aspects of its work.

172. In my view, this approach followed by Westinghouse is a sensible and effective way of addressing the requirements of the GDA Issue. The strengths of the extant design and safety case are highlighted and used to inform ALARP considerations, but it has not been used to limit the scope of the design options considered for providing additional flux detection.

173. The conclusion of the review of the primary and diverse protection available for heat removal and reactivity faults is the same as that reached by Ref. 22 for GI-AP1000-FS-03; it is only faults at shutdown that require additional flux protection to meet UK expectations for frequent faults. However, it is significant that Westinghouse came to that conclusion from its own systematic review of applicable faults, rather than relying on ONR (which defined the scope of GI-AP1000-FS-03) to identify which faults need to be considered. Although there is nothing new or unique in this part of Ref. 35, it does make it easy for me to assess Westinghouse's safety case positively against the expectations of SAPs FA.5 and FA.6.

174. Westinghouse summarises two phases of flux protection technology optioneering in Ref. 35. In its first pass (undertaken before it had completed its GI-AP1000-FS-03 work), it identified the following options:

- additional diverse ex-core detectors in the DAS

- sharing intermediate range ex-core detectors between the PMS and DAS
- nitrogen-16 (N-16) power monitoring
- fast-acting in-core detectors
- DAS high T_{hot} set-point optimisation

175. For each of these options, the additional protection that could be provided is discussed along with any disadvantages or difficulties with technology (eg lack of space, technology not mature yet, a risk of spurious initiation, etc).

176. In a second pass, undertaken after the GI-AP1000-FS-03 had been completed, a revised list of options were considered:

- N-16 power monitoring
- sharing intermediate range ex-core detectors between the PMS and DAS
- calorimetric temperature difference (ΔT RTDs)
- the extant in-core detectors
- sharing power range ex-core detectors between the PMS and DAS
- secondary system fault protection
    - low steam line pressure
    - high steam flow
    - high feedwater flow
    - high condenser pressure
- CVS system fault protection
    - boron meter
    - CVS flow meter (for inventory monitoring)

177. Again, Westinghouse identifies the protection each of these options could provide, and discusses the advantages and disadvantages of each.

178. I am satisfied that Ref. 35 shows that Westinghouse has undertaken a systematic and rigorous review of the potential options. Particularly noteworthy is that Westinghouse chose to utilise its internal Critical Issue Resolution Team (CIRT) process to consider the different options with a multi-disciplinary group of experts.

179. In a powerful but simple tabular presentation, Westinghouse has rated each option's ability to provide protection against the various increase in heat removal and reactivity faults as either:

- H – high likelihood of mitigating the consequences of the event
- L – theoretically could mitigate the event but not likely to be actuated
- N – judged to provide no protection

180. Significantly, Westinghouse states that this approach shows that there is no single option or set-point which has a high likelihood of protecting against all the events considered in GI-AP1000-FS-03. Regardless of whether GI-AP1000-FS-03 identified a shortfall in provision against UK expectations, if such an option existed it could well be an ALARP measure to implement. I agree with Westinghouse's conclusion that there is not a single 'perfect' option among the technologies it has considered.

181. Not included in Westinghouse's list of options is an improvement to the BEACON tool used for core monitoring in normal operations. Both ONR and Westinghouse recognised early on (indeed it is stated in the original wording of GI-AP1000-FS-04 Action 1) that it was not credible or desirable to increase the reliance on the software-based platform used by BEACON. With this established and accepted, it was possible for Westinghouse to make progress on the separate fuel design GDA Issue GI-AP1000-FD-03 "Use of the BEACON Code for On-line Compliance" (Ref. 21) without having to substantiate anything more than a modest reliability claim on the tool.

182. In my opinion, Westinghouse has given serious consideration in Ref. 35 to the option of using a sub-set of the extant in-core detectors used by BEACON for core flux mapping as input to some other C&I platform (notably the DAS) to provide additional protection against some of the faults considered. Such a consideration was a specific requirement of GI-AP1000-FS-04 Action 1. Westinghouse recognised that this option had the advantages of using existing sensors and could provide protection against the adverse power distribution faults that ONR identified in GDA Step 4 and prompted Action 1. However, it identified four main reasons for not pursuing it further:

- The extant in-core detectors are too slow to protect against rapid faults such as the steam line break events.
- Increasing the safety classification of the extant in-core detectors to Class 2 would be onerous.
- The extant in-core detectors work less effectively at low power levels, so further signal processing (amplification and filtering) would be required.
- The analogue platform of the (UK) DAS lacks the flexibility of a digital software-based platform (such as BEACON or the PMS) to perform the calculations required to detect power distortion faults.

183. Given my confidence in the rigour of Westinghouse's approach to optioneering in these cases and the information provided in Ref. 35, I am content to accept Westinghouse's conclusion that the extant in-core detectors, already included in the **AP1000** design and flagged by ONR in GDA Step 4 as a potential candidate system to meet UK expectations, are not a reasonably practicable option to pursue further. In its first pass at the optioneering stage, Westinghouse did consider fast-acting in-core detectors. However, Westinghouse believes the (schedule and licensing) risks of committing to this option outweigh the safety benefit (informed by the GI-AP1000-FS-03 work). Again, I am content with this reasoning.

184. ONR's original wording for GI-AP1000-FS-04 Action 1 (Ref. 4) mentioned that Sizewell B's primary protection system monitors the core power profile and margin to safe limits, and asked Westinghouse to consider whether improvements to the **AP1000** in-core flux monitoring systems to provide similar functionality could be a reasonably practicable improvement. Westinghouse has only partially addressed this point in Ref. 35, but I am content that the PCSR (when read alongside the GI-AP1000-FS-03 and GI-AP1000-FS-04 submissions) provides sufficient information for me to come to my own view on this point. Section 9.4.3 of the PCSR (Ref. 38) discusses:

- the approach to scheduling RCCA moves in banks;
- the mechanical and electrical systems used to move the RCCAs (which have some improvements compared with Sizewell B); and
- the means of detecting abnormal asymmetric power distributions and rod positions.

185. Crucially, and in contrast to Sizewell B, Westinghouse has been able to show that the **AP1000** reactor maintains a margin to the DNBR safety limit for even the most severe static RCCA misalignment faults (one RCCA is fully inserted, or where the mechanical shim or axial offset rod banks are inserted up to their insertion limit with one RCCA fully withdrawn while the reactor is at full power). Westinghouse has stated that this is possible because the fuel assembly design proposed for the **AP1000** reactor has intermediate flow mixing grids. This feature has resulted in a departure from nucleate boiling correlation that can support a high $F_{\Delta H}$ limit at full power, temperature and flow conditions. Cognisant of this information, and following consultation with colleagues in the fuel and core specialism considering very similar concerns as part of the assessment of GI-AP1000-FD-03 (Ref. 21), I am satisfied that additional protection against power distribution and DNBR margin challenges based on in-core flux detection is not needed.

186. Westinghouse has used the point on the limitations of the DAS to dismiss vanadium in-core detectors to eliminate several other detector options that would require some kind of processing. In principle, the technology of the DAS could be changed or a further protection system could be proposed. However, I recognise that going down this route would be onerous, time consuming, and almost certainly grossly disproportionate given the outcome of the GI-AP1000-FS-03 work. I acknowledge the appeal of providing additional functionality on an extant DAS rather than a new system, and while this may limit the options on what functions can be provided, it does shift the computation undertaken between sacrifice (money, time and trouble) and averting risk towards those options that are easier / more reasonably practicable to implement.

187. Having down-selected the list of options to those which could be implemented on the DAS, Westinghouse was left with three candidate approaches for faults occurring *at power*:

- N-16 flux monitoring for excessive increase in steam flow faults
- DAS high T_{hot} set-point optimisation for RCCA withdrawal faults and boron dilution faults
- negative flux rate trip on the DAS for dropped RCCA events

188. Westinghouse rejects the N-16 option in Ref. 35 on the basis that conservative analysis shows that any set-point higher than that of the primary protective measure (power range high neutron flux on the PMS at a high 118% of rated thermal power set-point) would never be reached by a frequent increase in steam flow fault, and therefore it would not provide any effective protection.

189. Westinghouse states that the UK **AP1000** DAS high T_{hot} set-point has already been optimised and changed from that considered in the standard plant DAS design as part of GDA Step 4 ATWS analysis, and no further change is desirable. Westinghouse is confident it has the balance between providing sufficient margin to DNBR limits and maximising the allowable operating margin.

190. Westinghouse finally goes on to state that the negative flux rate trip is not desirable because it would prevent the **AP1000** reactor's rapid power reduction system from working. This design feature allows the control system to drop sufficient RCCAs into the core to quickly reduce the rated thermal power by 60%. This allows the plant to stay online during full load rejections and partial feedwater pump trips. It argues that the small increase in safety that a DAS negative flux rate trip could provide is in gross disproportion to the negative impact on plant operations and the ability to recover from large load rejections.

191. I find all these arguments convincing. As a result, the only reasonably practicable design change Westinghouse has identified to provide diverse flux protection is automatic CMT actuation and dilution source isolation on the DAS for the shutdown boron dilution events (ie as considered in GDA Issue GI-AP1000-FS-03 Actions 6 and 7). From the review of Ref. 35, it is my judgement that this is an appropriate conclusion for Westinghouse to make.

4.7.2.2 Adequacy of Design Change Proposal APP-GW-GEE-5251

192. Having reached the conclusion that a design change to the DAS is necessary to meet UK expectations, Westinghouse has written and approved DCP APP-GW-GEE-5251 (Ref. 36) to incorporate it into the UK **AP1000** design and safety case documentation.

193. I am broadly content with Ref. 36. The fact that it has been written, approved and included within the latest versions of the design reference point (Ref. 23) gives me confidence that the change will be included in the UK **AP1000** design. It repeats the functional requirements established by Refs 22 and 35 for CMT injection and dilution

source isolation. More significantly, it goes on to demonstrate that Westinghouse has consulted widely, and appropriately internally, to understand the implications of the change on the safety case documentation, the design of the DAS, and on other systems, ahead of detailed design work being undertaken during site licensing.

194. A key factor in Westinghouse determining that this change was reasonably practicable was that both the intermediate range flux detectors and the DAS are already part of the **AP1000** design. In the extant design, the intermediate range flux detectors are connected to the Class 1 PMS to provide protection against uncontrolled RCCA bank withdrawal faults from subcritical or low power conditions. However, the fault schedule entry for this event (fault 1.15.1 in Ref. 39) and the supporting transient analyses assume that the PMS power range flux detectors can effectively protect against this event. I would characterise the position as being that the intermediate range flux detectors are *claimed* in the safety case as providing Class 1 protection against the identified fault, but Westinghouse has been able to *demonstrate* that the core is adequately protected by crediting the power range flux detectors in its supporting transient analysis without making any assumptions on the correct performance of the intermediate range flux detectors.

195. The design change does not propose to remove this functionality from the PMS. Instead, it is planned to split the signal for the intermediate range flux detectors such that it is shared between the PMS and DAS. However, this appears to challenge a key principle set out in SAP ESS.18 (Ref. 13) that C&I safety systems are physically separated and isolated from each other and do not share equipment.

196. During GDA Step 4 (ie long before this specific design change was proposed), ONR's C&I assessors identified some concerns about an apparent lack of diversity between the PMS and DAS. This resulted in GDA Issue GI-AP1000-CI-03 (Ref. 19) being written with a requirement for Westinghouse to provide a detailed diversity analysis for the two systems. Westinghouse has been working on addressing this GDA Issue since its return to GDA, in parallel with its work on the two fault studies GDA Issues discussed in this assessment report. This has resulted in Ref. 55 being submitted to ONR for assessment.

197. APP-GW-GEE-5251 (Ref. 36) has an obvious potential to impact the work being undertaken to address GI-AP1000-CI-03, so in consultation with C&I colleagues I raised two regulatory queries (Refs 56 and 57) directly asking Westinghouse if this change challenges C&I diversity and independence expectations and whether it had been included within the scope of Ref. 55.

198. Significantly, APP-GW-GEE-5251 did not identify Ref. 55 as a document impacted by the change. In its responses to the regulatory queries (Refs 56 and 57), Westinghouse attributed this to a matter of timing. The scope of Revision 0 of Ref. 55 was defined by design reference point Revision 7 (Ref. 23). APP-GW-GEE-5251 was only introduced into Revision 8 of Ref. 23. However, Ref. 55 was not issued until after the DCP was approved, so in accordance with Westinghouse's internal processes, it could not have been identified as an impacted document.

199. In Ref. 57, Westinghouse comments that it has undertaken a preliminary diversity assessment (outside Ref. 55) to evaluate if there are potential CCFs that could adversely affect both the PMS and DAS assuming that the change is implemented. It states that acceptable results have been obtained with two exceptions:

- A common point in the power distribution system has been identified which could affect the intermediate range, source range and power range channels.
- The potential for a PMS software CCF has been identified which could inadvertently place the intermediate range flux detectors into test mode, disabling the DAS protection.

200. In both cases, Westinghouse is confident that these weaknesses can be addressed later when the detailed design is completed during site licensing. Following discussions with specialist C&I colleagues, I am content with this strategy for taking the currently proposed design change forward. If these weaknesses can be addressed, I see little safety benefit in, for example, removing the intermediate range sensors from the PMS simply to meet ESS.18. By maintaining the functionality, it allows a different SAP, ESS.7, to be met ("all Class 1 protection systems should employ diversity in their detection of and response to fault conditions") for uncontrolled RCCA bank withdrawal faults at low power.

201. What is crucial for my judgement on the adequacy of Westinghouse's design change for GI-AP1000-FS-04 is evidence that the identified weakness are being tracked and will be addressed at the appropriate time in the future, given that neither APP-GW-GEE-5251 (Ref. 36) nor Revision 0 of the diversity analysis (Ref. 55) captured them. Working with my C&I colleagues, I secured the following assurances:

- Westinghouse's internal process for revising the list of documents impacted by a design change has been followed to include the diversity analysis (Ref. 55) as a document of relevance to APP-GW-GEE-5251.
- The change to the DAS will be included within the scope of Revision 2 of Ref. 55, with identified problems and potential solutions described.
- The requirement to resolve the issues during the detailed design phase will be included in the 'Safety Plan' provided as part of Revision 2 of the DAS Basis for the Safety Case (Ref. 49).

202. I have seen evidence that all of these actions have been taken. On that basis, I am content with Westinghouse's proposals for including within the UK **AP1000** design diverse flux protection on the DAS for shutdown faults which initiates automatic CMT actuation and dilution source isolation. I am also satisfied that the potential safety concerns associated with sharing the intermediate range flux detectors between the PMS and DAS have been appropriately considered, and steps have been taken ensure that the independence of the two systems is improved.

4.7.2.3 Assessment Conclusion for GI-AP1000-FS-04

203. Based on:

- my assessment of the main submission for GI-AP1000-FS-04 (Ref. 35);
- my investigations into Westinghouse's actions to implement the proposed design change to provide diverse flux protection on the DAS for shutdown faults;
- consideration of the work done by Westinghouse for GI-AP1000-FS-03;
- consultations with specialist colleagues in the C&I and fuel design topic area; and
- review of the PCSR (Refs 38 and 39),

I am satisfied that Westinghouse has effectively addressed the requirements and intent of the two actions of GI-AP1000-FS-04 and they can both be considered closed.

4.8 Assessment Findings

204. Assessment findings are matters that 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.

205. 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.

206. In my assessment I did not find any examples of matters which meet these criteria. There remains some UK-specific design work to be done beyond GDA to implement the proposed design change to the DAS, but I am content for this to be tracked and controlled through Westinghouse's and a future licensee's normal processes. However, I am satisfied that a regulatory tool is not required to ensure that this design work is completed.

207. In addition, the methodology proposed by Westinghouse in GDA Step 4 to demonstrate the resilience of the **AP1000** reactor to PCI failures (Ref. 62) needs to be applied to the RCCA misalignment faults considered in GI-AP1000-FS-03 Action 3. That methodology and the strategy for applying it during site licensing was considered back in GDA Step 4 and nothing in the assessment impacts the decisions made at the time.

5 CONCLUSIONS

208. This report presents the findings of the assessment of GDA Issues GI-AP1000-FS-03 and GI-AP1000-FS-04.

209. The requirements of the two GDA Issues were significant and wide ranging, for which Westinghouse has needed to undertake (and document) a significant amount of transient analysis, optioneering studies, and safety case justifications.

210. I have undertaken a detailed assessment of Westinghouse's key submissions, notably Refs 22, 33 and 35. I have also looked at how Westinghouse has incorporated a previously identified DCP (Ref. 30) into the **AP1000** safety case and design documentation, and the adequacy of the new DCP identified for GI-AP1000-FS-03 Actions 6 and 7 and GI-AP1000-FS-04. In addition, I have reviewed updated sections of the PCSR (Refs 38 and 39) for both background information and evidence that the results of the work for these two GDA Issues are reflected in the top-level safety case documentation.

211. For several of the actions, it has been necessary for me to consult and work with colleagues in other technical disciplines, notably C&I, electrical engineering and fuel design.

212. Ultimately, I am satisfied that:

- Westinghouse has undertaken all the necessary work required by the two GDA Issues.
- Westinghouse has generally been able to show that the **AP1000** reactor can meet the UK expectations for frequent faults without improvements to its flux protection systems.
- A modification is required to provide diverse protection for CVS failures in certain shutdown modes of operation.
- It is not reasonably practicable to make further enhancements to the **AP1000**'s flux protection system, including the modifications to the extant in-core flux measurement system identified by ONR in GDA Step 4 as a potential option.

213. No new matters have arisen for a future licensee to consider and take forward outside GDA as a result of my assessment of GI-AP1000-FS-03 and GI-AP1000-FS-04.

214. In summary, I am satisfied that GDA Issues GI-AP1000-FS-03 and GI-AP1000-FS-04 can be closed.

6 REFERENCES

1	Step 4 Fault Studies – Design Basis Faults Assessment of the Westinghouse AP1000 Reactor, ONR-GDA-AR-11-004a Revision 0, November 2011, TRIM 2010/581406
2	AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK, UKP-GW-GL-067 Revision 0, TRIM 2011/82011
3	GDA Issue “Diversity for Frequent Faults”, GI-AP1000-FS-03, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fs-03.pdf
4	GDA Issue “"Provision of Enhanced and Diverse Flux Protection to Protect against Adverse Power Distribution Faults”, GI-AP1000-FS-04, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fs-04.pdf
5	UK AP1000 Assessment Plan for Closure of GDA Fault Studies Issues 1 to 8, ONR-GDA-AP-14-002 Revision 0, March 2015, TRIM 2015/51535
6	GDA Issue “Design Reference Point and Adequacy of Design Basis Analysis”, GI-AP1000-FS-02, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fs-02.pdf
7	Step 4 Management of Safety and Quality Assurance Assessment of the Westinghouse AP1000® Reactor, ONR-GDA-AR-11-013 Revision 0, 11 November 2011, TRIM 2010/581518
8	ONR Guidance on Mechanics of Assessment, TRIM 2013/204124
9	GDA Guidance to Requesting Parties, www.onr.org.uk/new-reactors/ngn03.pdf
10	The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051 Revision 4, www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf
11	GDA Issue “PCSR to Support GDA”, GI-AP1000-CC-02 Revision 3, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf
12	Purpose and Scope of Permissioning, NS-PER-GD-014 Revision 5, TRIM 2015/304735
13	Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014, www.onr.org.uk/saps/saps2014.pdf
14	International Atomic Energy Agency (IAEA) Standards and Guidance: IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1, Revision 1, 2016 IAEA Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities, 2007 IAEA Safety Standards Series – Safety Guide: Safety Assessment and Verification for Nuclear Power Plants 2001 (this publication has been superseded by GSR Part 4 and SSG-2) www.iaea.org
15	Western European Nuclear Regulators Association: Reactor Safety Levels for Existing Reactors, September 2014

	WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010 Safety of New NPP Designs, March 2013 www.wenra.org
16	Review of the Applicability of Submitted UK AP1000 Design Basis Fault Modelling to the GDA Reference Design, GRS-ONR255-D1.2, February 2016, TRIM 2016/143232
17	GDA Issue "Adequacy of Safety Case for DAS", GI-AP1000-CI-01, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-ci-01.pdf
18	GDA Issue "DAS Adequacy of Architecture", GI-AP1000-CI-02, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-ci-02.pdf
19	GDA Issue "Diversity of PLS, PMS (inc CIM) and DAS", GI-AP1000-CI-03, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-ci-03.pdf
20	GDA Issue "PCSR Presentation of Claims Arguments and Evidence", GI-AP1000-EE-01, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-ee-01.pdf
21	GDA Issue "Use of the BEACON Code for On-line Compliance", GI-AP1000-FD-03, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fd-03.pdf
22	UK AP1000 Plant: Summary Report Supporting the Closure of the Fault Studies Issue 03, UKP-SSAR-GLR-002 Revision 0, May 2016, TRIM 2016/183955
23	AP1000 Design Reference Point for UK GDA, UKP-GW-GL-060 Revision 5, Reference Date 16 September 2010, TRIM 2011/560310 Revision 6, Reference Date 31 January 2015, TRIM 2015/201948 Revision 7, Reference Date 31 March 2016, TRIM 2016/227424 Revision 8, Reference Date 31 March 2016, TRIM 2016/378399 Revision 9, Reference Date 31 March 2016 TRIM 2016/446340 Revision 10, Reference Date 31 March 2016 TRIM 2017/18158
24	UK Generic Design Assessment: Evaluation of PCSR ATWS Scenarios for Design Reference Point, UKP-SSAR-GSC-210 Revision 0, TRIM 2016/183967
25	UK AP1000 Dropped Rod Diversity Analysis, UKP-SSAR-GSC-238 Revision 0, TRIM 2016/183992
26	UK AP1000 Boron Dilution Diversity Analysis, UKP-SSAR-GSC-239 Revision 0, TRIM 2016/184008
27	UK AP1000 Analysis of Excessive Load Increase ATWS Scenarios, UKP-SSAR-GSC-243, Revision 0, TRIM 2016/184018
28	UK AP1000 Complete Loss of Flow as a Result of Grid Frequency Perturbations, UKP-SSAR-GSC-247 Revision 0, TRIM 2016/184026
29	AP1000 PWR UK GDA Boron Dilution Analysis for Input to DAS Design Update, CN-AP1000-UK-014 Revision 0, TRIM 2016/184031
30	DAS PRHR Logic Change, APP-GW-GEE-1481 Revision 0, TRIM 2015/94213
31	APP-GW-GEE-1481 Implementation, Enclosure 1 to Westinghouse Letter WEC-REG-0229N, July 2015, TRIM 2015/287919

32	GDA Close-out for the AP1000 Reactor, GDA Issue GI-AP1000-FS-01: Spent Fuel Pool Safety Case, ONR-NR-AR-16-022 Revision 0, March 2017, TRIM 2016/274909
33	AP1000 Plant Chemical and Volume Control System (CVS) – Diversity Evaluation, UKP-GW-GL-165 Revision 0, TRIM 2016/180772
34	AP1000 Long Term Boration, VAT_DCP_000001 (Document ID: 1002486660, Version 01), February 2013, TRIM 2015/674
35	AP1000 Flux Protection and Diversity for Frequent Faults, UKP-GW-GL-083 Revision 0, June 2016, TRIM 2016/263885
36	Addition of Diverse Protection for Boron Dilution at Shutdown, APP-GW-GEE-5251 Revision 0, June 2016, TRIM 2016/289669
37	AP1000 Pre-Construction Safety Report, UKP-GW-GL-793 Revision 0, March 2011, TRIM 2011/192251
38	AP1000 Pre-Construction Safety Report, UKP-GW-GL-793: Chapter 9 Revision 0B, October 2016, TRIM 2016/407251
39	AP1000 Pre-Construction Safety Report, UKP-GW-GL-793: Chapter 8 Revision 0C, October 2016, TRIM 2016/411261
40	US NRC Regulations 10CFR 50.62: Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants, www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0062.html
41	Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor, UKP-GW-GLR-016 Revision B, October 2010, TRIM 2011/82101
42	AP1000 Safety Analysis Checklist (SAC) & Future Limits, UKP-SSAR-F5-001 Revision 0, July 2016, TRIM 2016/278732
43	UK Fault Studies Analysis Basis, UKP-SSAR-GLR-001 Revision 0, August 2016, TRIM 2016/333118
44	AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, March 2011, TRIM 2011/81804
45	GDA Close-out for the AP1000 Reactor, GDA Issue GI-AP1000-FS-02: Design Reference Point and Adequacy of Design Basis Analysis, ONR-NR-AR-16-023 Revision 0, March 2017, TRIM 2016/274911
46	Changes to Diverse Actuation System (DAS) Voting Logic and Associated Architecture, APP-GW-GEE-2286 Revision 0, March 2011, TRIM 2015/128080
47	Changes to Diverse Actuation System (DAS) Platform Implementation, APP-GW-GEE-2287 Revision 0, March 2011, TRIM 2015/128084
48	GDA Issue “Fault Schedule for AP1000”, GI-AP1000-FS-08, www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fs-08.pdf
49	United Kingdom AP1000 United Kingdom AP1000 Basis of Safety Case for the Diverse Actuation System, UKP-DAS-GLR-001: Revision 0, November 2010, TRIM 2011/81957 Revision 1, July 2016, TRIM 2016/296907 Revision 2, December 2016, TRIM 2016/484831
50	IEC 61513:2011 “Nuclear Power Plants. Instrumentation and control for systems important to safety. General requirements for systems”, International Electrotechnical Commission (IEC)

51	Complete UK Grid Electrical Code, www2.nationalgrid.com/UK/Industry-information/Electricity-codes/Grid-code/The-Grid-code/
52	Confirmatory Technical Questions to Support the Assessment of UKP-GW-GL-165, RQ-AP1000-1660, TRIM 2016/346702
53	Step 4 Fuel and Core Design Assessment of the Westinghouse AP1000 Reactor, ONR-GDA-AR-11-005 Revision 0, November 2011, TRIM 2010/581526
54	Queries Prompted by ONR Assessment of GI-AP1000-FS-03 Action 7: Adequacy of the ANC Code, RQ-AP1000-1705, TRIM 2016/386093
55	United Kingdom AP1000 Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS), UKP-GW-GLR-023: Revision 0, June 2016, TRIM 2016/255845 Revision 1, November 2016, TRIM 2016/435951 Revision 2, December 2016, TRIM 2016/502495
56	Clarification on DCP APP-GW-GEE-5251 Revision 0 in relation with GI-AP1000-CI-03 and GI-AP1000-FS-03/04, RQ-AP1000-1647, TRIM 2016/355078
57	Comments on the Diversity Analyses (GI-AP1000-CI-03, UKP-GW-GLR-023 Revision 0 and UKP-GW-GLR-024 Revision 0), RQ-AP1000-1672, TRIM 2016/380907
58	UK AP1000 PWR Dropped Rod Fault Studies, CN-AP1000-UK-001 Revision 0, February 2016, TRIM 2016/347677
59	T/H Evaluation of ATWS Dropped Rod Statepoints for UK AP1000, CN-AP1000-UK-003 Revision 0, TRIM 2016/347683
60	Transient Analysis for DBAs in Nuclear Reactors, NS-TAST-GD-034 Revision 3, July 2016, www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-034.pdf
61	Queries Prompted by ONR Assessment of GI-AP1000-FS-03 Action 3: Dropped Rod Diversity Analysis, RQ-AP1000-1684, TRIM 2016/386087
62	Westinghouse Response to Regulatory Observation (RO-AP1000-050): Demonstration of Protection against PCI Fuel Failure, Revision 0, 2010, TRIM 2011/93165

Annex 1 – Summary of the GDA Issues' Actions

GI-AP1000-FS-03: Diversity for frequent faults, Ref. 3

Action	Summary
Action 1	Implement the revised moderator temperature coefficients assumed in the ATWS analysis reported in UKP-GW-GLR-016 within the AP1000 safety analysis checklist document WCAP-9272-P-A.
Action 2	Demonstrate protection for the excessive increase in secondary steam flow fault at full power for both the case with successful reactor trip and the case with failure of the reactor to trip due to either mechanical failure of the rods to insert or failure of the reactor protection system. Or Propose design changes to provide protection against the excessive increase in secondary steam flow faults.
Action 3	Demonstrate the provision of diverse protection against rod misplacement faults including one or more dropped rods. Or Propose design changes to protect against the consequences of such a fault.
Action 4	Implement the proposed modification to provide a high hot leg temperature trip on the Diverse Actuation System to protect against the RCCA bank withdrawal fault at full power with failure of the PMS.
Action 5	Demonstrate protection against a complete loss of forced flow fault as a result of perturbations in grid frequency for both the case with successful reactor trip and the case with failure of the reactor trip due to either mechanical failure of the rods to insert or failure of the reactor protection system.
Action 6	Demonstrate the provision of diverse protection against loss of CVS following a normal reactor trip and xenon decay including demonstration of diversity to operator action. Or Provide a consequence analysis demonstrating the acceptability of the design against HSE's [*now ONR's*] accident frequency targets.
Action 7	Analyse the homogenous boron dilution fault occurring in shutdown conditions with failure of the protection and monitoring system to demonstrate that there is diverse protection against the fault.

GI-AP10000-FS-04: Provision of enhanced and diverse flux protection to protect against adverse power distribution faults, Ref. 4

Action	Summary
Action 1	Westinghouse is required to provide a report demonstrating a comprehensive assessment of the potential for enhancing the protection provided by installed in-core instrumentation against adverse power distribution faults.
Action 2	Westinghouse is required to demonstrate that diverse protection is provided against frequent reactivity and power distribution faults such as the excessive increase in secondary steam flow and rod misalignment faults. Consideration should be given to the possibility of enhancing the installed in-core instrumentation to provide diverse protection against these faults.