Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Fault Studies – Design Basis Faults Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-004a
Revision 0
21 November 2011

COPYRIGHT

© Crown copyright 2011

First published December 2011

You may reuse this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view the licence visit www.nationalarchives.gov.uk/doc/open-government-licence/, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email psi@nationalarchives.gsi.gov.uk.

Some images and illustrations may not be owned by the Crown so cannot be reproduced without permission of the copyright owner. Enquiries should be sent to copyright@hse.gsi.gov.uk.

Unless otherwise stated, all corporate names, logos, and Registered® and Trademark™ products mentioned in this Web site belong to one or more of the respective Companies or their respective licensors. They may not be used or reproduced in any manner without the prior written agreement of the owner(s).

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.

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND) or the Nuclear Installations Inspectorate (NII) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000® reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires Westinghouse to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the AP1000® reactor.

EXECUTIVE SUMMARY

This report presents the findings of the Fault Studies assessment of the design-basis fault analyses for the AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the European Design Control Document (EDCD) and the supporting documentation submitted by Westinghouse during Step 4.

This assessment has followed a step-wise approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by Westinghouse were examined, and in Step 3 the arguments that underpin those claims were examined.

The scope of the Step 4 assessment was to review the safety aspects of the AP1000 reactor in greater detail, by examining the evidence, supporting arguments and claims made in the safety documentation, building on the assessments already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the design-basis fault analyses contained within the EDCD and the supporting documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific, or generic, weaknesses in the safety case. The areas identified for sampling in Step 4 were set out in advance in an assessment plan based upon the findings of the Step 3 report.

My assessment has focussed on:

- The design-basis analyses performed in support of the AP1000. The assessment has been subdivided into a number of individual fault areas covering faults where the integrity of the primary circuit is maintained (such as steamline break faults, loss of feed faults, loss of flow faults, and reactivity faults), and Loss of Coolant Accidents (LOCA), where the integrity of the primary circuit is lost due to a break occurring somewhere on the primary circuit. Faults occurring during shutdown conditions or faults occurring away from the reactor in the spent fuel pool have also been considered.
- The validation of the computer codes which are used to model design-basis faults. In addition to assessing the validation evidence provided by Westinghouse, independent confirmatory analysis has been commissioned in selected cases from technical support contractors using alternative computer codes and analysts. This work, which is valuable for reaching judgements on the adequacy of the Westinghouse's codes and analysis, is summarised in this report.

It should be noted that the assessment of the fuel and core design, a technical area closely related to Fault Studies, is reported separately. As a result, the justification of the fuel safety limits during accident conditions, including assessment of the critical heat flux correlations needed to demonstrate fuel integrity during many of the fault transients, is not discussed in any detail in this report.

The design-basis thermal-hydraulic analysis of the containment environment during fault conditions, such as a large-break loss of coolant accident or a main steamline break, is also reported separately; the assessment of the severe accident analyses performed by Westinghouse is covered by the same report.

It has been agreed with Westinghouse that it is more appropriate to assess the proposed Technical Specifications, the emergency operating procedures, and the site-specific radiological consequence assessments during the site licensing process. Hence these items are outside the scope of the GDA process and are not discussed within this assessment.

In some areas lack of detailed information has limited the extent of my assessment. As a result HSE-ND will need additional information to underpin my judgements and conclusions: these are identified as Assessment Findings to be carried forward as normal regulatory business and are listed in Annex 1. Some of the findings identified within this report are of particular significance and will require resolution before the HSE would agree to the commencement of the nuclear safety related stage of construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues and each one will require an associated Resolution Plan proposed by Westinghouse.

The range of faults considered to be within the design basis within the EDCD does not meet UK requirements. A number of drafts of a Pre-construction Safety Report (PCSR) were provided during GDA but these too did not meet the UK requirements for a design-basis safety case. Westinghouse recognises this and has responded by producing a substantially revised PCSR in March 2011. However, this has arrived too late for assessment during Step 4. For this reason, HSE-ND has raised a cross-cutting GDA Issue requiring Westinghouse to submit the revised PCSR for assessment. This assessment will need to be completed before Consent will be granted for the commencement of safety-related construction of the nuclear island. Nevertheless, in my judgement the information provided in the EDCD, supplemented with the supporting documents provided in response to Regulatory Observations (RO) and Technical Queries (TQ) raised during Step 4, is adequate to enable a characterisation of the fault conditions on the AP1000 for the purposes of this Step 4 assessment.

From my assessment, I have concluded that:

- Westinghouse has improved the design basis safety case for the AP1000 through the additional analysis performed in response to the regulatory observations raised in my Step 3 report. It has been able to extend the design basis to demonstrate that the design is tolerant to passive single failures at the functional level. Westinghouse has also extended the design basis to cover complex situations in which a combination of events may initiate a fault sequence, although this is an area where there is further work still to be done and a number of GDA Issues has been raised in respect of this.
- The analytical work performed by Westinghouse has been aided by a number of important design changes to the reactor protection system on the AP1000 that in my opinion will significantly improve the safety of the design. These changes have been proactively identified by Westinghouse. The design changes identified are:
    - An upgrading of the following active systems to Category A Class 2 safety systems: the Diverse Actuation System (DAS), the Start-up Feedwater system (SFW), the normal Residual Heat Removal system (RNS), the Component Cooling Water system (CCS), the essential service water system, and the stand-by diesel generators. In particular, the RNS has been upgraded from a single train to a two-train system at the point of injection into the Direct Vessel Injection (DVI) lines; the DAS has been upgraded from a 2-out-of-2 to a more fault tolerant architecture involving dual 1-out-of-2 and partial 2-out-of-3 system.
    - Implementation of a modification to alter the set-point for the isolation of the SFW and the Chemical and Volume Control system (CVS) on High Steam Generator (SG) level alarm signal to improve protection against a Steam Generator Tube Rupture (SGTR) fault by increasing the margin to overfill on the affected Steam Generator (SG).
    - Implementation of a reactor trip signal on the DAS to trip the reactor on high hot-leg temperature.
    - Implementation of a reactor trip signal to mitigate the effects of an inadvertent actuation of the Passive Residual Heat Removal (PRHR) Heat Exchanger.

  - Implementation of a modification to enable the P-17 interlock to prohibit rod withdrawal following a spurious drop fault of one or more rods.

- In addition, Westinghouse has committed to the implementation of a blocker device on the Automatic Depressurisation System (ADS) to reduce the likelihood of spurious actuation. There is also a commitment to improvements in the design of the spent fuel pool although the safety cases justifying these design changes have still to be developed.

The full list of GDA Issues I have identified during my assessment requiring additional work from Westinghouse is:

- Completion of the safety case is required for the spent fuel pool setting out the claims identified during Step 4 of GDA and providing the supporting arguments and evidence for those claims. The design-change process needs to be followed to incorporate the various physical modifications identified and all the affected documents need to be updated.
- Westinghouse is to demonstrate that, for all design basis faults, the submitted design basis analysis is appropriate for the agreed GDA design reference point and that all safety claims are supported by the analysis. If this cannot be done with pre-existing analysis, new analysis could be required. The final PCSR produced for GDA is to summarise this analysis for all design basis faults. A complete and consistent set of core design limits reflecting the design basis fault analysis is required.
- Westinghouse to implement design modifications and provide further analysis to demonstrate functional diversity for faults with an initiating frequency greater than 1×10^{-3} per year.
- Westinghouse need to examine the feasibility of enhancing the flux protection on the AP1000 to provide automatic and diverse protection against frequent adverse power distribution faults possibly using the current design of in-core instrumentation.
- Westinghouse is to examine whether it is reasonably practicable to enhance the design of the RNS system in its role as the diverse safety injection system on the AP1000.
- Westinghouse is to provide validation evidence that the In-containment Refuelling Water Storage Tank (IRWST) is functionally capable of cooling the PRHR system during intact circuit faults for 72 hours.
- Westinghouse is required to complete a fully integrated design basis safety case for shutdown faults in the PCSR.
- Westinghouse is to present its updated fault schedule.

In my opinion, based upon the information provided in the EDCD and supporting documentation submitted as part of the GDA process, there are no fundamental reasons for believing that a satisfactory safety case cannot be made for the generic AP1000 reactor design, subject to satisfactory progression and resolution of GDA Issues during the forward work programme for this reactor. A major item of work will be to assess the revised PCSR. It must also be recognised that some of these GDA Issues may ultimately require changes to the plant design. It is therefore too early to rule out the need for changes to plant layout or the provision of additional safety systems.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
AFCAP	Advanced First Core Analysis Programme
ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
ATWT	Anticipated Transient without Trip
BMS	(Nuclear Directorate) Business Management System
BOC	Beginning of Cycle
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
C&I	Control and Instrumentation
CAMP	Code and Maintenance Programme
CCS	Component Cooling Water System
CHF	Critical Heat Flux
CMF	Common Mode Failure
CMT	Core Make-up Tanks
CSARP	Cooperative Severe Accident Research Project
CVCS	Chemical and Volume Control System (Sizewell B)
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DCD	Design Control Document
DDS	Data Display and Processing System
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DVI	Direct Vessel Injection
EBS	Emergency Boration System
ECS	Emergency Charging System
EDCD	European Design Control Document
EOC	End of Cycle
FPS	Fire Protection System
GDA	Generic Design Assessment
GRS	Gesellschaft fűr Anlagen- und Reaktorsicherheit
HHSI	High Head Safety Injection
HSE	The Health and Safety Executive
HVAC	Heating, Ventilation, Air Conditioning
IAEA	The International Atomic Energy Agency
ICRP	International Commission on Radiological Protection

LIST OF ABBREVIATIONS

IRS	Incident Reporting System
IRWST	In-containment Refuelling Water Storage Tank
LBLOCA	Large Break Loss of Coolant Accident
LCO	Limits and Conditions for Safe Operation
LOCA	Loss of Coolant Accident
MAAP	Modular Accident Analysis Program
MBLOCA	Medium Break Loss of Coolant Accident
MDEP	Multi-National Design Evaluation Programme
MFW	Main Feedwater System
MOV	Motor Operated Valve
MOX	Mixed Oxide Fuel
MSIV	Main Steam Isolation Valve
MSSV	Main Steam Safety Valve
ND	The (HSE) Nuclear Directorate
NII	Nuclear Installations Inspectorate (now the Office for Nuclear Regulation)
OECD-NEA	Organisation for Economic Cooperation and Development – Nuclear Energy Agency
ONR	Office for Nuclear Regulation
OSU	Oregon State University
PCCWST	Passive Containment Cooling Water Storage Tank
PCI	Pellet-Clad Interaction
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PIRT	Phenomena Identification and Ranking Table
PLS	Plant Control System
PMS	Protection and Monitoring System
PORV	Power Operated Relief Valve
POSRV	Pilot Operated Safety Relief Valve
PPS	Primary Protection System
PRHR	Passive Residual Heat Removal Heat Exchanger
PSA	Probabilistic Safety Analysis
PSV	Pressuriser Relief Valves
PWR	Pressurised Water Reactor
PXS	Passive Core Cooling System
RAPFE	Radial Averaged Peak Fuel Enthalpy
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System

LIST OF ABBREVIATIONS

REA	Rod Ejection Accident
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
RPV	Reactor Pressure Vessel
SAP	Safety Assessment Principle
SBLOCA	Small Break Loss of Coolant Accident
SFS	Spent Fuel Cooling System
SFW	Start-up Feedwater System
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SPS	Secondary Protection System
SSC	Structures, Systems and Component
SWS	Service Water System
TAG	Technical Assessment Guide
TQ	Technical Query
TSC	Technical Support Contractor
US NRC	United States Nuclear Regulatory Commission

TABLE OF CONTENTS

Annexes

1 INTRODUCTION

1 This report presents the findings of the Fault Studies assessment of the design basis analyses for the AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The intention was for the assessment to have been carried out on the December 2009 version of the Pre-construction Safety Report (PCSR, Ref. 12). However, the quality of this document did not meet regulatory expectations and so the decision was made for the assessment to instead focus upon Revision 1 of the European Design Control Document (EDCD), Ref. 16) supplemented by supporting evidentiary information derived from the Master Submission List (Ref.14). The approach taken was to assess the principal submission, i.e. the EDCD, and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of the Nuclear Directorate (ND) Business Management System (BMS) procedure AST/001 (Ref. 2). The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 In addition to and as result of the assessment of the EDCD and its supporting references, a number of Technical Queries (TQ) and Regulatory Observations (RO) were issued. The responses made by Westinghouse to the TQs and ROs were assessed against the same principles.

3 The strategy and scope adopted for this Fault Studies assessment are set out in Section 2. The basis of Westinghouse's safety case is summarised in Section 3. My assessment of Westinghouse's safety case, with more details on the safety case for specific faults, is presented in Section 4. The conclusions of this Fault Studies assessment are presented in Section 5.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR DESIGN BASIS FAULT ANALYSIS

2.1 Assessment Plan

4 The intended assessment strategy for GDA Step 4 of the Fault Studies area was set out in an assessment plan (Ref. 1). This assessment plan, which is based upon the findings from the GDA Step 3 report, identifies the intended scope of the assessment and the standards and criteria to be applied. This assessment strategy is summarised in the following sub-sections:

2.2 Standards and Criteria

5 Judgements have been made against the 2006 HSE SAPs for Nuclear Facilities (Ref. 4). In particular, the fault analysis and design basis accident SAPs (FA.1 to FA.9), the severe accident analysis SAPs (FA.15 to FA.16), the assurance of validity SAPs (FA.17 to FA.22), the numerical target SAPs (NT.1, Target 4, Target 7 to Target 9) and the engineering principles SAPs (EKP.2, EKP.3, EKP.5, EDR.1 to EDR.4, ESS.1, ESS.2, ESS.7 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4) have been considered. Westinghouse has assessed the safety case against its own design requirements.

2.3 Assessment Scope

6 It is seldom possible or necessary to assess a safety case in its entirety. Sampling is used to limit the areas scrutinised, to limit the total effort to be applied, and to improve the overall efficiency of the assessment process. If sampling is done in a focused, targeted and structured manner it can be expected to reveal generic weaknesses in the safety case as a whole. The majority of samples are drawn from areas of high safety relevance since weaknesses in these areas are potentially very serious, but a few should also be taken from lower significance areas to check for possible omissions within the safety case

7 The Fault Studies assessment has focused on the design basis analysis of the AP1000 which has been sub-divided into a number of individual fault areas. These assessments are reported in Section 4 of this report and cover faults where the integrity of the primary circuit is maintained (such as steamline break faults, loss of feed faults, loss of flow faults, and reactivity faults), and Loss of Coolant Accidents (LOCA), where the integrity of the primary circuit is lost due to a break occurring somewhere on the primary circuit. Section 4 also reports on faults occurring during shutdown conditions or faults occurring away from the reactor in the spent fuel pool. In contrast with GDA Step 3, a major area of assessment in GDA Step 4 has been a review of the validation of the computer codes which play a significant part in these analyses. In particular, in selected cases independent confirmatory analysis has been commissioned from technical support contractors and this work is reported in detail in this report.

8 It should be noted that the assessment of the fuel and core design, which is a technical area that is closely related to Fault Studies, is not reported here but in a separate report (Ref. 17). As a result, the justification of the fuel safety limits during accident conditions, including assessment of the critical heat flux correlations needed to demonstrate fuel integrity during many of the fault transients are not discussed in detail in this report.

9 The design basis thermal hydraulic analysis of the containment building during fault conditions, such as a Large Break Loss of Coolant Accident (LBLOCA) or a main steam line break, are also reported separately (Ref. 18). The assessment of the severe accident analyses performed by Westinghouse is also covered by the same report and is therefore

not discussed in any detail in this report. The assessment of the Probabilistic Safety Analysis (PSA) is also reported separately (Ref. 19).

10 The principal document considered in the Fault Studies area is Revision 1 of the EDCD (Ref. 16). The main chapter I have assessed is Chapter 15 but I have also assessed other sections as necessary. In GDA Step 3, Revision 0 of the EDCD was assessed. The chapters relevant to Fault Studies were not significantly changed by the update to Revision 1, with the notable exception of the new descriptions of the upgraded normal Residual Heat Removal system (RNS), Spent Fuel Pool cooling system (SFS) and Component Cooling Water system (CCS) designs. It was through the work done in GDA Step 3 that the areas for specific focus in GDA Step 4 were identified. It was also through the work done in Step 3 that the initial areas for independent analysis by Technical Support Contractors (TSC) were identified.

11 In addition to the EDCD, the responses to ROs and TQs received during GDA Step 4 have been subject to detailed assessment. The expectation is that the responses to ROs and some TQs together with information from the EDCD will be reflected in a future substantial revision to the PCSR. However, the revised version of the PCSR (Ref. 13) was only received at the end of March 2011, which was too late for assessment.

2.3.1 Findings from GDA Step 3

12 The Step 3 assessment report (Ref. 6) concluded that there are no fundamental reasons for believing from a Fault Studies perspective that a satisfactory safety case for AP1000 could not be made. However the range of faults considered within the EDCD was less comprehensive than desired and a number of the comments and ROs were made that required resolution in GDA Step 4.

13 In particular, the report noted the importance of the performing sensitivity studies in which input information is varied on the basic assumptions made within the fault analyses as an aid to judgement on the adequacy of the analysis. While some information of this kind was available, more comprehensive sensitivity analyses was necessary in some areas. Furthermore, the design basis analyses are only concerned with single events as initiators of a fault sequence. Attention also needed to be paid to complex situations in which a combination of events may initiate a fault sequence.

14 Specific findings included:

- Westinghouse was requested to demonstrate that the list of design basis initiating events was complete, including faults at shutdown and on the spent fuel pool. The list of design basis initiating faults was to be reconciled with those of the PSA. A design basis safety case was required for each fault (RO-AP1000-46).
- Westinghouse was requested to review all design basis initiating events with a frequency of greater than 1×10^{-3} per year and demonstrate that a diverse safety system, qualified to an appropriate standard, was provided for each safety function. The single failure criterion was also to be extended to include passive failures (RO-AP1000-47).
- Westinghouse was requested to perform a radiological consequence assessment for each design basis fault against Target 4 of the safety assessment principles (RO-AP1000-48).
- With regard to the proposal to use the BEACON reactor physics code to demonstrate on-line compliance with the fuel safety Technical Specifications, Westinghouse was

requested to show that a diverse method exists for the operator to ensure compliance (RO-AP1000-49).

- Westinghouse was requested to demonstrate that fuel is protected from pellet-clad interaction (PCI) failure for frequent faults. The feasibility of connecting the in-core detectors to the reactor protection system was also to be considered (RO-AP1000-50).
- Westinghouse was requested to include Anticipated Transient without Trip (ATWT) faults within the design basis. An As Low As Reasonably Practicable (ALARP) justification for not installing an emergency boration system was required (RO-AP1000-51).
- For each fault, Westinghouse was requested to provide evidence that the plant can reach a safe shutdown state from each controlled state (RO-AP1000-52).
- The assessment of large-break loss-of-coolant accidents compares the fuel cladding temperatures expected against safety limits. Westinghouse was requested to include within its analysis detailed consideration of the potential for fuel channel blockage caused by features of the transient such as plastic buckling of spacer grids (RO-AP1000-53).
- Westinghouse has made a case for the retention of core material in the vessel should the core melt in a severe-accident. Westinghouse was requested to perform a further examination of this research (RO-AP1000-68).

15 These significant findings were captured as ROs for which Westinghouse has undertaken additional work and submitted additional documentation during Step 4. These findings have been specific areas of focus within Step 4 of GDA and are discussed in this report with the exceptions of RO-AP1000-49 and RO-AP1000-50 which are discussed in the fuel and core assessment report (Ref. 17) and RO-AP1000-68 on in-vessel retention which is discussed in Ref. 18.

16 During the course of the GDA Step 4 assessment, HSE-ND raised concerns about the possibility of the protection and monitoring system (PMS) spuriously actuating the Automatic Depressurisation System (ADS). Westinghouse was requested to identify any additional measures to reduce the frequency of this event. This was identified as an additional RO (RO-AP1000-82). In addition, the requirement to explore the feasibility of connecting the in-core detectors to the reactor protection system, originally identified in RO-AP1000-50, was further clarified through an additional Regulatory Observation (RO-AP1000-91).

2.3.2 Additional Areas for Step 4 Assessment

17 Additional areas for further investigation for Step 4 were identified in the assessment plan. These areas have been assessed using already available safety submissions (principally the EDCD (Ref. 16) and its supporting references), the responses to TQs raised during GDA Step 4 and through technical discussions held with Westinghouse. In particular, the assessment plan identified five areas that were not assessed in Step 3 that needed to be assessed during Step 4:

- assess the thermal hydraulic analysis undertaken to support the PSA success criteria;
- assess the appropriateness and validity of the computer codes used in accordance with SAPs FA.17 to FA.24;

- commission TSCs to undertake independent confirmatory analysis of selected AP1000 transients;
- support to the assessment of the internal and external hazards safety cases, and;
- assess the safety case arguments and thermal hydraulic analysis of the containment response to design basis fault sequences which result in primary and secondary steam releases to the containment building.

18 The intention at GDA Step 3 was to review the thermal hydraulic analysis supporting the PSA success criteria during GDA Step 4. In practice an alternative strategy has been adopted in which the thermal hydraulic success criteria have been reviewed by a TSC (GRS – see Section 2.3.3 below) working for the PSA technical leads within HSE-ND. The work performed by GRS is reported in Ref. 20 and the PSA assessment is reported in Ref. 19. Hence, the PSA success criteria are not discussed further within this report.

19 The assessment of computer codes used by Westinghouse has been undertaken in GDA Step 4 and is reported in Section 4 on a case-by-case basis. In addition to looking at evidence to support Westinghouse's own codes, valuable judgements can be drawn by comparing the results from its codes against independent analyses of the same events undertaken by TSCs using alternative codes (see Section 2.3.3 below).

20 Support has been provided to external and internal hazard topic leads in GDA Step 4 and is reported in Section 4. Finally, as noted in Section 2.3.1, the thermal hydraulic analysis supporting the design basis assessment of the containment response to fault conditions has been an area for assessment in GDA Step 4 but is reported in Ref. 18.

2.3.3 Use of Technical Support Contractors

21 TSCs have been utilised in GDA Step 4 to support the HSE-ND assessment of the AP1000. These have principally been used to undertake independent confirmatory analysis of transient analysis studies performed by Westinghouse. Ultimately, it is for Westinghouse to demonstrate the adequacy of its safety case. However, analysis undertaken by independent analysts using a different computer code can provide additional confidence in a safety case if the results obtained are comparable with those of Westinghouse.

22 Gesellschaft fűr Anlagen-und Reaktorsicherheit (GRS) mbH undertook the most amount of work in GDA Step 4 in the Fault Studies area. It completed projects in the following areas:

- Development of a reactor physics model for AP1000 (Ref. 21).
- Development of a thermal hydraulic model for AP1000 (Refs 22 and 23).
- ATWT analysis using the developed reactor physics and thermal hydraulic models (Ref. 24).
- Cooldown fault analysis using the developed reactor physics and thermal hydraulic models (Ref. 25).
- Review of passive safety systems (Refs 26 and 27) including sensitivity studies to key parameters governing the performance of the Core Make-up Tanks (CMT), and the sizing of the ADS-4 valves and In-containment Refuelling Water Storage Tank (IRWST) during small-break LOCA faults and an uncertainty assessment of key parameters following a Direct Vessel Injection (DVI) line break fault.

23 The analyses undertaken with the independently developed models are discussed in Sections 4.2.2, 4.2.3, 4.2.5 and 4.2.8 respectively. The reactor physics and thermal hydraulic codes used by GRS are its own "in-house" codes and are independent of those used by Westinghouse.

24 AMEC has been used to undertake independent confirmatory analysis of Small Break Loss of Coolant Accidents (SBLOCA) faults and Steam Generator Tube Rupture (SGTR) faults. HSE-ND provided AMEC with a United States Nuclear Regulatory Commission (US NRC) model of the AP1000 developed for the TRACE thermal hydraulic code. AMEC modified this model to reflect design basis assumptions set out in the EDCD and supporting references, and to model the specific fault conditions. The results of this work are discussed in Section 4.2.8.5.

25 The HSE SAPs (Ref. 4) set out numerical targets for the calculated radiological consequences for design basis fault sequences. In the EDCD (Ref. 16), Westinghouse has presented radiological consequences for fault sequences. However the analysis follows a methodology prescribed by US NRC and is compared against dose limits set out in US NRC's 10 CFR 50.34 (a US Code of Federal Regulation) and Regulatory Guide 1.183. No attempt is made to compare against Target 4 in the HSE SAPs. As a result, RO-AP1000-48 was issued at the end of GDA Step 3 requiring Westinghouse to reassess the radiological consequences (for a generic UK site) and make the appropriate UK comparisons. AMEC has performed a review of the new analysis, the conclusions of which are discussed in Section 4.6. It should be noted that site-specific calculations of radiological consequences are beyond the scope of GDA (see Section 2.3.6).

2.3.4 Cross-cutting Topics

26 Fault analysis, by its very nature, tends to interface with many of the technical areas associated with a safety case. However, a number of areas have been identified as "cross-cutting topics". Of these, the following have involved fault analysis assessment effort and are discussed within this report:

- categorisation and classification of structures, systems and components (see Section 4.1.4);
- spent fuel pool faults (see Section 4.2.11);
- radiological source terms (see Section 4.6), and;
- limits and conditions of safe operation (see Section 4.8).

2.3.5 Integration with Other Assessment Topics

27 Specific key areas for co-ordinated work are:

- review of the Westinghouse assessment method for calculating radiological consequences following design basis fault sequences (in collaboration with radiation protection and chemistry topic leads);
- assessment of thermal hydraulic analysis undertaken to support PSA success criteria (in collaboration with the PSA topic lead);
- assessment of the categorisation and classification of Control and Instrumentation (C&I) systems (in collaboration with the C&I topic lead);
- assessment of thermal hydraulic analysis undertaken to support structural analysis (in collaboration with the structural integrity topic lead);

- review of the design and sizing requirements of key safety components, e.g. heat exchangers, safety injection pumps etc (in collaboration with mechanical engineering topic lead);
- assessment of the internal and external hazards safety case (in collaboration with the internal and external hazards topic leads), and;
- assessment of the spent fuel pool design, including the design of the racks, piping and cooling systems (in collaboration with many topic areas).

2.3.6 Out of Scope Items

28 The following items have been agreed with Westinghouse as being outside the scope of GDA:

- Site-specific calculations for radiological consequences – these will be provided as part of nuclear site licensing. Westinghouse has provided radiological consequences for a generic site for comparisons with Target 4 of the SAPs.
- Technical Specifications – Technical Specifications for the reactor are presented in the EDCD but these have not been assessed in GDA. It is for a future operator to produce definitive Technical Specifications and Emergency Operating Procedures.
- Operation with Mixed Oxide Fuel (MOX) in the reactor or the fuel handling facilities is outside the scope of GDA.
- As part of routine operations, the AP1000 is designed for the primary circuit inventory to be at “mid-loop” during shutdown. Faults from this state are presented in the EDCD and have been assessed as part of GDA. However, the EDCD does not present a sufficient safety case for Steam Generator (SG) or squib valve maintenance activities with the fuel still in the core. Future operators will have a choice of either undertaking such maintenance activities with the fuel removed from the reactor vessel or developing a safety case for undertaking such activities at “mid-loop” with the fuel still loaded. Assessment of such maintenance operations is therefore outside the scope of GDA.

3 WESTINGHOUSE'S SAFETY CASE

29 The basis of Westinghouse's safety case in the Fault Studies area is that the design of the AP1000 is capable of preventing a significant release of radioactive materials during normal operation and design basis accidents and that the PSA demonstrates that the residual risk from accidents beyond the design basis has been reduced to as low as is reasonably practicable.

30 In order to achieve these objectives, Westinghouse claim to have incorporated the following features into the design of the AP1000:

- The reactor core is designed so its nuclear characteristics do not contribute to a divergent power transient and that there is no tendency for divergent oscillations of any operating characteristic, considering the interaction of the reactor with other plant systems.
- Safety systems are provided to mitigate design basis accidents by ensuring prompt reactor shutdown and the removal of decay heat. Westinghouse claims that these systems are provided with sufficient redundancy and independence so that no single failure of active components can prevent their successful operation.
- A key design requirement of the AP1000 is that the Class A1[1] safety systems will operate automatically when required regardless of the availability of off-site power supplies, the normal generating system and the on-site standby diesel generators. Indeed, Westinghouse claims that for every design basis fault on the AP1000 there is an automatic Class A1 system to mitigate the fault without the need for operator action for 72 hours. For this reason, the systems are designed to maximise the use of natural driving forces such as pressurised nitrogen, gravity flow and natural circulation flow coupled with the use of an automatic depressurisation system. A minimum number of valves are used for the purpose of initially aligning the safety systems.
- The design of Class A1 safety systems does not use active components such as pumps, fans or diesel generators and support systems such as diesel-backed alternating current, component cooling water, service water, heating, ventilation and air conditioning.
- The design of nuclear safety systems and engineered safety features is capable of withstanding natural environmental disturbances such as earthquakes, floods, and storms at the station site.
- The fuel handling and storage facility is designed to prevent inadvertent criticality and to maintain shielding and cooling of spent fuel.
- The containment vessel which completely encloses the reactor system will, in conjunction with other engineered features, limit the release of radioactivity from inside the containment, in the event of a design basis accident.
- Provisions are made for passively removing energy from the containment vessel following accidents. The passive containment cooling system maintains the integrity of the containment vessel by ensuring that the pressure and temperature of the

[1]Westinghouse defines a Class A1 system as a system that performs a Category A safety function using Class 1 SSCs. A Category A safety function is a principal means of maintaining nuclear safety while the Class 1 SSCs provide the principal means of fulfilling a Category A safety function.

containment remains within the appropriate design limits in the event of a design basis accident.

31 Westinghouse claims that the significant innovation with the AP1000 is the provision of the Passive Core Cooling System (PXS) to provide core cooling following design basis accidents. The PXS provides core residual heat removal, safety injection, and depressurisation without the use of active equipment such as pumps and ac power sources.

32 The PXS uses three sources of water to maintain core cooling through safety injection. These injection sources are the CMTs, the accumulators, and the IRWST. These injection sources are directly connected to two nozzles on the reactor vessel so that injection flow is not lost following a break on the hot or cold legs of the Reactor Coolant System (RCS).

33 The CMTs replace the high-pressure safety injection systems in conventional Pressurized Water Reactors (PWR). They provide high pressure injection of borated water if the normal make-up system is inadequate or is unavailable. They are filled with borated water in two parallel trains which are designed to function at any reactor coolant system pressure using gravity and the temperature and height differences from the reactor coolant system cold leg as the motivating forces. These tanks are designed for full RCS pressure and are located above the RCS loop piping. A pressure balance line connects one of the cold legs to the top of the CMT and an outlet line connects the bottom of the CMT to the DVI line.

34 The accumulators are similar to those found in conventional PWRs. They are large spherical tanks approximately three-quarters filled with cold borated water and pre-pressurized with nitrogen. The accumulator outlet line is connected to the DVI line. A pair of check valves prevents injection flow during normal operating conditions. When system pressure drops below the accumulator pressure (plus the check valve cracking pressure), the check valves open allowing coolant injection to the reactor downcomer of the reactor vessel via the DVI line.

35 Depressurisation is provided by the PXS using a four stage ADS to permit a relatively slow, controlled, RCS pressure reduction. The ADS lowers the pressure of the RCS so that the accumulators and later the IRWST can inject cold borated water into the reactor core. The ADS consists of sixteen valves divided into four depressurization stages. These stages connect to the RCS at three locations. The ADS first, second and third stage valves are connected to the nozzles on top of the pressuriser. Each stage consists of two trains of valves. The first stage opens on low CMT liquid level. ADS Stages two and three open shortly after the first stage on timers. The flashing coolant that is discharged out of ADS Stage one, two and three valves is directed to the IRWST by means of spargers.

36 The fourth-stage valves are connected by two redundant paths to each reactor coolant loop hot leg (i.e. 4 valves in total). The ADS-4 system is operated by explosive squib-valves, discharging directly to the containment atmosphere.

37 The IRWST is a large pool filled with borated water within the containment building. One of its (safety) functions is to provide low-pressure injection for the RCS. The IRWST has two injection lines connected to the DVI lines. These flow paths are normally isolated by two squib valves in parallel. When the primary pressure drops below the head pressure of the water in the IRWST, the flow path is established through the DVI into the reactor vessel downcomer. The IRWST water is sufficient to flood the lower containment compartments to a level above the reactor vessel head and below the outlet of the ADS Stage-4 lines.

38 The PXS also includes one Passive Residual Heat Removal (PRHR) heat exchanger. It is designed to remove decay heat from the RCS following an accident. The PRHR heat exchanger is located in the IRWST at an elevation above the reactor core. The inlet to the heat exchanger is connected to one of the two hot legs while the outlet is connected to the outlet plenum on one of the two steam generators. The inlet is open to the RCS pressure, and the outlet pipe is normally closed by two isolation valves in parallel to assure that the system is protected against a single active failure. During normal operation, the water in the heat exchanger tubes is in thermal equilibrium with the IRWST. When a safety injection signal is generated following an accident, these isolation valves are opened and natural circulation is established in the heat exchanger which is sized to remove the decay heat from the RCS. To enhance natural circulation, the reactor coolant pumps are tripped on a safety injection Safeguard (S) signal.

39 The Passive Containment Cooling System (PCS) is a passive safety system which provides heat removal from the containment shell to the environment via natural circulation air and water flow from the Passive Containment Cooling Water Storage Tank (PCCWST) by the force of gravity. It serves as the means of transferring heat to the ultimate heat sink for events resulting in a significant increase in containment pressure and temperature.

40 The AP1000 has three separate main Control & Instrumentation (C&I) systems that perform duty plant control and monitoring, response to transients, and response to design basis accidents:

- The Protection and Safety Monitoring system (PMS) provides detection of off-nominal conditions and actuation of Class A1 systems necessary to achieve and maintain the plant in a safe shutdown condition.
- The Diverse Actuation System (DAS) is an additional safety system (Class A2 system) that provides an alternative means to PMS of initiating reactor trip, actuating selected safety systems and providing plant information to the operator. It provides a number of diverse automatic actuations in support of Category A safety functions, but it can also be actuated manually, providing a diverse way to initiate selected safety systems
- The Plant Control system (PLS) provides the functions necessary for normal operation of the plant from cold shutdown through to full power. The PLS also contributes to the delivery of Category A safety functions in response to transients; parts of the system are therefore classified as Class A2.

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR DESIGN BASIS FAULT ANALYSIS

41 My assessment against the SAPs of the Fault Studies aspects of the AP1000 design basis analysis is presented below.

42 The assessment commences in Section 4.1 with a review of the general aspects of the AP1000 safety case that apply across all faults.

- Section 4.1.1 considers the fault categorisation system that has been applied by Westinghouse to the AP1000.
- Sections 4.1.2 to 4.1.5 cover the approach to diversity and common mode failure, redundancy and the single failure criterion, and the implications of these on the categorisation and classification of structures, systems, and components important to safety and how the AP1000 moves from the controlled state reached following activation of the safety systems in response to a fault condition to the long-term safe shutdown state.
- Section 4.1.6 considers the general structure of Westinghouse's safety case.
- Section 4.1.7 looks at how Westinghouse has demonstrated that the list of initiating faults it has identified is systematic, auditable and comprehensive.

43 Section 4.2 constitutes the major portion of the report, presenting a systematic assessment of each of the main fault classes in turn, sampling a selection of key initiating faults, linking each with an assessment of the associated fault sequences. The related transient analysis aimed at demonstrating the functionality of the safety systems claimed to provide protection against the fault is reviewed.

44 In Section 4.3, an assessment of the validation evidence for the passive safety systems for non-LOCA faults together with the LOFTRAN computer code used to perform most of the transients analysis studies is presented. Likewise, in Section 4.4, an assessment of the validation evidence for the passive safety systems for LOCA faults together with the NOTRUMP and WCOBRA/TRAC computer codes is presented. Section 4.5 complements these sections with a review of the potential thermal hydraulic failure modes of the passive safety systems.

45 Section 4.6 reviews the radiological consequences analysis of the bounding faults. Section 4.7 provides an overview of the assessment while Section 4.8 reviews how the limits and conditions identified from safety analysis will be captured in future updates of the safety case.

46 Section 4.9 discusses how Fault Studies assessment will provide support to the ongoing structural integrity assessment. Section 4.10 assesses the adequacy of Fault Schedule which aims to summarise the totality of AP1000 design basis safety case.

47 The final two sections discuss commissioning requirements resulting from the Fault Studies assessment and summarises the areas where HSE has co-operated with overseas regulators.

48 In some areas lack of detailed information has limited the extent of my assessment. As a result HSE-ND will need additional information to underpin my judgements and conclusions and these are identified as Assessment Findings to be carried forward as normal regulatory business. These are listed in Annex 1.

49 Some of the findings identified in Section 4 of this report are of particular significance and will require resolution before HSE-ND would agree to the commencement of nuclear

safety-related construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues are listed in Annex 2.

4.1 General Aspects of AP1000 Safety Case

4.1.1 Fault Categorisation

50 The design basis analysis presented in Chapter 15 of the EDCD (Ref. 16) classifies plant conditions into four categories according to the anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:

- Condition I: Normal operation and operational transients.
- Condition II: Faults of moderate frequency.
- Condition III: Infrequent faults.
- Condition IV: Limiting faults.

51 Westinghouse's aim is to demonstrate that no fuel rod failures occur for condition I and II events. Condition III and IV events may result in limited fuel rod failure but should not result in the release of radioactive material above the dose limits specified by the US NRC in 10 CFR 50.34. These differ from the dose limits given in SAPs FA.3, FA.7 and Target 4. For this reason, Westinghouse has revised its radiological assessment to meet UK requirements. An assessment of the revised Westinghouse methodology including a discussion about its appropriateness for comparison with Target 4 is given Section 4.6.

4.1.2 Diversity and Common Mode Failure

52 SAP EDR.2 requires that appropriate use should be made of diversity within the designs of Structures, Systems and Components (SSC) important to safety, while SAP EDR.3 states that common mode failure should be explicitly addressed. In my GDA Step 3 report, I noted that the fault categorisation scheme discussed above is based upon the ANSI N18.2 standard (Ref. 15), which dates from 1973. This guide has been superseded by a latter version produced in 1983 (Ref. 28). It is noticeable that the categorisation scheme only considers single events as initiators of a fault sequence. It does not consider complex situations in which a combination of events may initiate a fault sequence.

53 In the UK, it is considered good practice to consider any fault sequence with a frequency greater than 1×10^{-7} per year to be within the design basis (Ref. 7). This is the approach adopted for Sizewell B. Given that SAP EDR.3 limits the reliability claim that may be placed on any safety system to be no better than 1×10^{-5} per demand, this means that for any initiating frequency greater than 1×10^{-2} per year (and in practice for most initiating frequencies greater than 1×10^{-3} per year) a diverse safety system, qualified to an appropriate standard, is required to be provided for each safety function and the functional capability of the system needs to be demonstrated using design basis analysis techniques with appropriate safety margins included to cover for uncertainties. For this reason, RO-AP1000-47 was raised requiring Westinghouse 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 safety function. This extension to the design basis analysis will need to be included within a revision of the PCSR.

54 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has produced a matrix table in which each of the frequent design basis initiating faults are listed against a series of safety functions for the reactor and the spent fuel pool. This matrix is then used to identify

the bounding frequent fault transient for each safety function. For those transients not already covered by a design basis analysis, an additional fault transient has been analysed in response to RO-AP1000-47 (or RO-AP1000-51 in the case of ATWT events). These extensions to the design basis analysis will need to be included within a revision of the PCSR.

55 In performing this work, Westinghouse has identified the following Category A[1] safety functions for the AP1000:

Facility	Safety Function
Reactor	Reactor Trip Sensor
	Essential Safety Function Sensor
	Short-term Reactivity Control
	Long-term Reactivity Control
	Decay Heat Removal
	RCS Pressure Control
	RCS Inventory Control
	Containment Cooling
	Containment Isolation
	Ultimate Heat Sink
	Control & Instrumentation
	Electrical Power
Spent Fuel Pool	Essential Safety Function Sensor
	Reactivity Control
	Decay Heat Removal
	Ultimate Heat Sink
	Control & Instrumentation
	Electrical Power

56 For each safety function and for each frequent fault, Westinghouse claims to have identified a “primary” and a “diverse” back-up means of mitigating the event. The diverse means would be relied upon in the unlikely event of a Common Mode Failure (CMF) of the primary means. Westinghouse notes that in selecting the diverse feature, its general approach has been to minimise the importance of the active systems. Hence, where there is a choice between a diverse passive feature and a diverse active feature, the diverse passive feature has been designated the “diverse” means of mitigation.

57 Westinghouse acknowledges that determination of whether two features are diverse is based upon engineering judgement. In some cases where there may be some question

[1] The SAPs define a Category A safety function as any function that plays a principal role in ensuring nuclear safety while a Category B safety function that makes a significant contribution to nuclear safety.

as to whether sufficient diversity is provided, Westinghouse claim that discussion is provided to justify the diversity. In particular, if a feature (or part of a feature) is listed as both the primary and the diverse means, then another feature (typically an active feature) is identified as an additional "other" means. Where this is the case, it is my judgement that HSE-ND should regard these "other" means as providing the diverse safety function within the design basis safety case with the appropriate consequences for control of their availability within the Technical Specifications, in-service testing, inspection and maintenance during the site licensing process.

58 Westinghouse notes that the primary and diverse backup lists of components should not be viewed as being two separate groups as no single CMF could fail all the primary equipment. However, even though the primary and diverse lists do not need to be treated as separate groups, in some cases Westinghouse has chosen to do so in order to minimise the number of transient analysis cases that have had to be performed. These additional analyses are reviewed together with the relevant original design basis analysis on a case-by-case basis in the relevant fault specific discussion in Section 4.2 below. As a result of this work, Westinghouse has identified the need for a design change to the DAS to provide an additional trip signal on high hot leg temperature. This change is discussed in Section 4.2 and is captured within the GDA Issue on functional diversity, under **GI-AP1000-FS-03** as Action 4.

4.1.3 Redundancy and the Single Failure criterion

59 SAP EDR.2 also requires that appropriate use should be made of redundancy within the designs of SSCs important to safety while SAP EDR.4 requires that no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. SAP FA.6 requires that design basis fault sequences should include consideration of single failures.

60 In my GDA Step 3 report, the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 were discussed with regard to passive single failures because of the definition of the design criterion used by Westinghouse. Westinghouse's design criteria (Ref. 30) require passive failures to be considered within the single failure criterion only after a period of 24 hours following an initiating event. Westinghouse generally considers the failure of a non-return valve (also called a check valve) to change position as an active failure. However, in a few special cases justification for not considering the failure of a non-return valve was made in the design. In contrast, in the UK, passive failures are considered within the single failure criterion (Ref. 31). These are assumed to be caused or revealed as a result of the transient. In addition, the failures of a non-return valve to open on demand and of a steamline isolation valve to close on demand are considered as active and not passive failures in the UK. For this reason, RO-AP1000-47 (Ref. 10) also required Westinghouse to perform a review of each design basis fault on the AP1000 to identify whether there are any passive failures on the safety systems that will prevent a safety function from being performed successfully.

61 In its response to RO-AP1000-47 (Ref. 32), Westinghouse claim to have reviewed all safety systems on the AP1000 with regard to passive single failures. Westinghouse claims to demonstrate that the design is generally able to tolerate a passive single failure at the functional level as required by SAPs EDR.2 and EDR.4. However, the response to RO-AP1000-47 (Ref. 32) has identified the following areas where a passive single failure could potentially affect the performance of a safety function and for which it is required to demonstrate that the position is ALARP (as low as is reasonably practicable):

- Intact circuit fault with single passive failure of the normally open PRHR inlet isolation Motor Operated Valve (MOV) or the normally open manual isolation outlet valve resulting in loss of PRHR Heat exchanger.
- Double ended DVI line small break LOCA with single passive failure of the normally open IRWST isolation MOV resulting in loss of intact IRWST flow path.
- Double ended DVI line small break LOCA with single passive failure of the intact CMT normally open check valve to re-open after closing resulting in loss of intact CMT injection capability.
- Double ended DVI line small break LOCA with single passive failure of the intact accumulator check valve resulting in loss of intact accumulator injection capability.
- Large Break LOCA with single passive failure of one accumulator check valve resulting in loss of accumulator injection capability from 1 of 2 accumulators.

62 The adequacy of the response to RO-AP1000-47 on passive single failures in general (Ref. 32) and the specific analysis of the passive single failures listed above is assessed on a case-by-case basis in Section 4.2 below. In particular, the single passive failure of the PRHR isolation valve is reviewed within Section 4.2.3 on reduction in heat removal faults and also within Section 4.2.8 on decrease in reactor coolant inventory faults for the case of a small break LOCAs (SBLOCA). The other passive single failures are also discussed in Section 4.2.8. There are two additional single passive failures that Westinghouse does not appear to have considered explicitly within the RO-AP1000-47 response. These are failure of the Pressuriser Safety Relief valve (PSV) to re-close on demand resulting in a consequential LOCA, which is discussed in Section 4.2.3, and failure of a Main Steam Isolation Valve (MSIV) to close on demand following an SGTR, which is discussed in Section 4.2.8.

4.1.4 Categorisation and Classification of Structures, Systems and Components

63 It is noted that in the EDCD the standard US approach to safety classification is presented. The passive safety systems (along with their C&I) which are claimed against design basis faults are all identified as “Safety-Related” systems. Active systems are typically “Non-safety” systems and are not claimed in the design basis analysis presented in Chapter 15 of the EDCD. However, for the AP1000, Westinghouse did perform as part of the AP1000 design process a systematic review of the active defence in depth systems to determine their safety importance. As a result of this assessment additional regulatory oversight was applied to these systems on a selective basis.

64 During GDA Step 4, Westinghouse has developed a safety classification system (Refs 33 and 34) more consistent with the UK SAPs (Ref. 4). SAP ECS.1 sets the expectation that safety functions should be categorised based on their safety significance. Safety function categorisation should then be used as part of the method to classify SSCs delivering safety functions.

65 Westinghouse has followed this approach to some extent. Westinghouse has defined a Category A safety function (the highest category) to be one which is utilised to achieve and maintain a non-hazardous stable state for at least 72 hours following the initiating event. This means that almost all the safety functions of interest in design basis fault analysis are Category A.

66 Under Westinghouse’s new system, the AP1000 passive safety systems are classified as Class A1 safety systems (i.e. a Class 1 system delivering a Category A safety function listed in Section 4.1.2 above). It follows that the passive systems are designed to achieve

and maintain a stable state for at least 72 hours. Active systems performing a safety role are classified as Class A2 safety systems. In the context of Westinghouse's approach to demonstrating diversity for frequent faults, Westinghouse notes that the primary means of achieving a Category A safety function is required to be classified as a Class A1 safety system. The diverse back-up means does not have to be Class A1 and can be Class A2. Westinghouse's Class B2 system is a Class 2 system that forms the principal means of implementing a Category B function.

67 As a result of the ROs in the Fault Studies area, notably RO-AP1000-47 on the need to demonstrate diversity, the UK safety case for AP1000 design basis faults now makes formal claims on Class A2 active systems in what Westinghouse regards as limited cliff-edge events. This is not reflected within the EDCD design basis analysis but it is understood that it will be reflected within the PCSR design basis analysis as part of the "frequent faults diversity" assessment. This represents a potential problem with the AP1000 UK Safety Categorisation and Classification Methodology (Ref. 34), upon which the AP1000 UK Safety Categorisation and Classification of Systems, Structures and Components (Ref. 33) is based, since it still refers to the EDCD for the definition of the UK AP1000 design basis analysis whereas this needs to be revised to reflect the extension to the design basis analysis performed in response to RO-AP1000-47 (Ref. 29). For example, at the start of Appendix A of the methodology report (Ref. 34) it is stated that the active systems do not provide accident mitigation capability credited in the design basis accident analysis unless their operation makes the consequences of an accident more limiting. Clearly, the work performed in response to RO-AP1000-47 (Ref. 29) contradicts this statement. Assessment Finding **AF-AP1000-FS-01** requires any future licensee to revise the methodology report (Ref. 34) in line with this observation and ensure that the Categorisation and Classification report (Ref. 33) remains consistent with the outcome.

68 In practice, this may not be a problem, in that, as noted above, Westinghouse appears to have pragmatically reclassified those active systems identified as important to safety in accordance with the results of a "focused" PSA analysis (Ref. 34) as Class A2 safety systems within the Categorisation and Classification report (Ref. 33). I have reviewed the proposed Categorisations and Classifications for the Mechanical, Electrical, C&I and Structures SSCs presented in the Categorisation and Classification report (Ref. 33) and the results appear to be sensible. One possible exception is the PLS which is classified as a Class B2 safety system while in the diversity review (Ref. 29) this is claimed to be a Class A2 safety system. Assessment Finding **AF-AP1000-FS-02** has been raised requesting any future licensee to reconcile this contradiction in the categorisation although it is recognised that the engineering standards applied are in practice determined by the classification and not the categorisation.

69 A related matter is that the Categorisation and Classification report (Ref. 33) only recognises the plant control functions provided by the PLS. It is unclear what is the classification of those parts of the PLS system that allow operator actuation of Class A2 safety systems such as the RNS. Assessment Finding **AF-AP1000-FS-03** has therefore been raised for a future licensee to confirm that those parts of the PLS that are being claimed for manual operator intervention to initiate Category A safety functions are also classified as Class A2.

70 The UK AP1000 Safety Categorisation and Classification Methodology report (Ref. 34) also discusses how classification affects control of plant availability and inspection, testing and maintenance requirements. It is considered that these aspects of the safety case will be more appropriately dealt with during the site licensing process and so the Technical Specifications are regarded as being outside the scope of GDA. Additionally,

the Technical Specifications reported in Chapter 16 of the EDCD do not take account of any of the work performed during GDA, including the responses to ROs such as RO-AP1000-47 and RO-AP1000-51.

71 For these reasons, the Technical Specifications presented in the EDCD have not been assessed during GDA. Nevertheless, it should be emphasised that in the UK all limits and conditions identified within the safety case, including control of availability requirements, need to be captured within the Operating Rules and these are all potentially subject to regulatory oversight. These limits and conditions should be primarily identified from the design basis assessment presented in the safety case, supplemented by risk reduction insights gained from the PSA where appropriate. However, reference to investment protection considerations is inappropriate for safety case documentation.

4.1.5 Controlled and Safe Shutdown States

72 For most reactor design basis faults, there are two distinct periods after the initial fault to consider. There is usually an initial crisis period where safety limits (e.g. fuel safety limits and plant temperature and pressure limits) are challenged while the safety systems are triggered and act to mitigate the fault. After this early crisis period has passed and a controlled state has been reached, it is necessary to progress to and maintain a non-hazardous state in the long term (for AP1000 this taken to be 72 hours), known as the safe shutdown state.

73 In Chapter 15 of EDCD (Ref. 16), Westinghouse has systematically presented transient analysis to demonstrate for the design basis faults considered that there are margins to the safety limits as the controlled state is reached. This is supplemented by the response to RO-AP1000-47 (Ref. 29), which shows how these limits are respected for frequent faults with diverse safety systems. The EDCD does discuss the plant features that would automatically bring the plant to the safe shutdown state for the two general classes of events (non-LOCA and LOCA). However, neither the EDCD nor the response to RO-AP1000-47 (Ref. 29) systematically set out the safety case on how to take the reactor from the controlled state to the safe shutdown state for each fault (i.e. they do not identify what safety systems are required and then demonstrate with transient analysis that the claimed safety systems can deliver the necessary functions).

74 In my Step 3 GDA report (Ref. 6), RO-AP1000-52 (Ref. 10) was raised for Westinghouse to demonstrate for all design basis faults that a safe state could be reached. For frequent faults this includes the need to identify the diverse systems that are required to achieve this state. Westinghouse has provided a response (Ref. 35) in which it reviews all the reactor faults considered in the response to RO-AP1000-46 discussed below. For each fault it attempts to identify the systems required to provide the following four basic safety functions:

- reactivity control;
- decay and sensible heat removal to the ultimate heat sink;
- reactor coolant system inventory control, and;
- reactor coolant system pressure control.

75 On the basis of these studies, Westinghouse claims that there is a Class A1 means to reach the safe shutdown state for all the faults considered. Furthermore, for intact circuit faults, SGTR faults and the more frequent LOCA faults, it claims that additional Class A1 or A2 systems are available to provide diversity. These claims in the response to

RO-AP1000-52 are assessed in detail on a case-by-case basis for each of the main fault classes in Section 4.2 below.

76 However, it is worth noting that as part of its argument, Westinghouse has defined what it regards as a safe shutdown state for the AP1000 as requiring a reactivity condition (K_{eff}) less than 0.99 and an average RCS temperature less than 215.6°C. No technical justification is given for this definition representing a safe state. In particular, the choice of 0.99 appears incorrect since the Technical Specification shutdown margin justified in the EDCD is 1600 pcm corresponding to a K_{eff} of 0.984 which is lower than the Westinghouse target even before calculational uncertainties in the transient analysis are taken into account. Furthermore, it does not include a limit on RCS pressure so the definition appears to be incomplete. For this reason, Assessment Finding **AF-AP1000-FS-04** has been raised requiring a future licensee to develop an adequate justification of the safe shutdown state and to demonstrate that the safety systems claimed by Westinghouse are capable of meeting these requirements.

4.1.6 Structure of the Safety Case

77 The design basis accident analyses for the AP1000 are presented within Chapter 15 of the EDCD with the exception of the containment design basis analyses, which are presented in Chapter 6, and the spent fuel pool design basis analyses, which are presented in Chapter 9. A summary of the results of the thermal hydraulic analyses that underpin the PSA success criteria is presented in Chapter 6 and Appendix A of the UK AP1000 Probabilistic Risk Assessment (Ref. 36). The latter also includes an assessment of faults that occur during shutdown operations for which no design basis analysis is presented within the EDCD. Overall, I judge that the extent of analysis largely meets the requirements of SAP FA.1 which requires that fault analysis should be carried out comprising design basis analysis, probabilistic safety analysis and severe accident analysis; although in some areas, such as shutdown faults and analysis aimed at demonstrating diversity, additional analysis will be required.

78 Nevertheless, while the transient analysis presented in the EDCD forms an important element of the evidence required for a design basis safety case, it does not by itself constitute an adequate safety case. In the US regulatory system (in which the AP1000 was developed) the Chapter 15 DCD analysis demonstrates that the US NRC safety criteria have been met. In the UK, by contrast, it is for the licensee / RP to identify the safety criteria and demonstrate that they have been met in such away that the claims, arguments and evidence are all presented in an adequate safety case.

79 Westinghouse has produced a PCSR for GDA, attempting to provide this additional information to supplement that provided in the EDCD. However it arrived at the end of the GDA Step 4 assessment period and has not been assessed in the fault studies area. Clearly, this needs to be done at some point in the future. Given the prominent role the transient analysis previously occupied in the EDCD, some aspects of this assessment will be straightforward. However, the safety case structure, the claims and arguments and the use of transient analysis will have to be looked at for the first time since this will all be new information.

80 Specific areas of the PCSR for assessment in the Fault Studies topic area will be:

- How the list of initiating events has been extended beyond that considered in the EDCD.
- How the UK categorisation and classification system (Ref. 33) and the demonstration of diversity has been applied to the fault studies area.

- How new transient analysis and extensions to the design basis scope have been incorporated into the PCSR.
- How the compliance with Target 4 of the SAPs has been demonstrated for the radiological consequences of design basis fault sequences.
- The adequacy of the Fault Schedule and how it summarises and complements the design basis safety case.

81 From the discussions held with Westinghouse during GDA Step 4 and through the review of RO responses, it is anticipated that the new UK Fault Studies safety case presented in the PCSR will contain new safety claims that were not identified in the EDCD (in particular where the design basis safety case has been extended or as a result of the new categorisation and classification system). It needs to be established how these new claims are cascaded beyond the Fault Studies sections of the PCSR to other sections (e.g. new claims on C&I, electrical systems, tolerance against hazards etc). Hence, on the basis of this current assessment, and so excluding consideration of the revised PCSR (Ref. 13), Cross-cutting assessment topic area GDA Issue **GI-AP1000-CC-02** has been raised on Westinghouse to provide an adequate PCSR (Ref. 144). In practice, Westinghouse has already submitted to HSE-ND the revised PCSR, so averting a potential action to do so. However, HSE-ND will still need to assess the revised PCSR before this GDA Issue can be closed out.

4.1.7 Fault Identification

82 SAP FA.2 requires that the process for identifying initiating faults should be systematic, auditable and comprehensive. In my GDA Step 3 report, I noted that the AP1000 list of design basis faults did not appear to include support system faults and control and protection faults. It was not clear therefore that the list of faults was comprehensive. In contrast, the list of initiating events for the PSA presented in Chapter 15 of the EDCD was based upon a systematic failure modes effects analysis of the AP1000 systems. Recognising that, in principle, any initiating event identified in the PSA should be included within (or bounded by) a design basis initiating event unless it is screened out on the basis of low frequency (as acknowledged by SAP FA.5), I raised RO-AP1000-46 (Ref. 10) requesting Westinghouse to reconcile the list of design basis initiating events with the list of PSA initiating events with the aim of demonstrating that the list of design basis initiating events considered within the EDCD was as comprehensive as possible.

83 For its response to RO-AP1000-46 (Ref. 37), Westinghouse has provided a revised (composite) fault list which enables a comparison of the list of design basis initiating events against the list of PSA initiating events to be performed. It also includes a list of additional faults not considered in either list. The response reviews loss of coolant accidents, transients (including loss of RCS flow faults, power excursion faults, loss of feed faults, loss of condenser faults, and secondary-side breaks), support system failures (loss of component cooling water, loss of service water, loss of offsite power and loss of compressed air), shutdown faults, and non-reactor faults including spent fuel pool faults. I&C (C&I) faults are generally grouped within other fault classes according to the consequences of the fault. The scope of the Westinghouse review appears to be comprehensive apart from internal and external hazard initiating events that are not considered in any detail within the document.

84 Internal and external hazards are discussed further in Sections 4.2.13 and 4.2.14 below. Westinghouse has traditionally handled such events separately from the design basis fault analysis. This approach may be acceptable, but it is important for ensuring good visibility of the safety case that these initiating events are at least included within the Fault

Schedule (notably for hazards there should be visibility of the categorisation and classification of the safety barriers that protect against identified events). Hence, under GDA Issue **GI-AP1000-FS-08**, Westinghouse will be expected to include these items within the Fault Schedule.

85 Reviewing the design basis fault list against the PSA list presented in the composite fault list given in the table in Appendix A of the RO-AP1000-46 response (Ref. 37), it is clear there are a number of PSA events that are not explicitly bounded by an equivalent design basis event. However, the final column of the table makes it clear that many of these events are bounded by a more limiting design basis fault. There are five exceptions. These are rupture of the Reactor Pressure Vessel (RPV), interfacing system LOCA events, consequential LOCA (due to spurious stuck open PSV), consequential SGTRs and inadvertent operation of the pressuriser heaters.

86 Westinghouse argues that rupture of the Reactor Pressure Vessel and interfacing system LOCA events are beyond design basis events. While it is accepted that this is the case for the first of these events, the argument for the interfacing system LOCA events is based upon the sequence frequency assuming protection is provided by isolation valves being able to isolate the breach and not the initiating frequency of the break. Given that such events can potentially by-pass containment, the claim on these isolation valves needs to be considered within a design basis assessment and appropriately categorised and classified. For this reason, Assessment Finding **AF-AP1000-FS-05** has been raised requesting a future licensee to provide a design basis safety case for these interfacing system LOCA events.

87 Westinghouse has provided additional arguments in its responses to TQ-AP1000-837 and TQ-AP1000-838 (Ref. 9) and claims that consequential SGTR faults and consequential LOCA faults are adequately bounded by other existing design basis events. These additional arguments for consequential SGTR faults and consequential LOCA faults are respectively discussed in Sections 4.2.2 and 4.2.3 below. In its response to TQ-AP1000-1099 (Ref. 9), Westinghouse argues that inadvertent operation of the pressuriser heaters is protected by a high pressuriser pressure trip signal and that the rate of pressure increase is bounded by the turbine trip case. These additional arguments are discussed further in Section 4.2.10 below.

88 Clearly, comparison of the design basis list of faults with the PSA list of faults only ensures comprehensive fault coverage within the design basis if the PSA list of faults is complete. The PSA assessment of the AP1000 (Ref. 19) has identified a number of initiating events that are not adequately covered within the PSA list of faults. Some of these problems are because the PSA has conservatively bounded some faults rather than explicitly considering them within the PSA. This is generally not a problem for the design basis assessment providing the assumed frequency of the bounding initiating event reflects the higher frequency of those less onerous faults that it is claimed to bound. Examples include loss of feed to one SG and PRHR tube rupture events. Other events are clearly beyond the design basis (e.g. consequential steamline break of the second SG following steamline break on the first SG inside containment). Still other events that have not been considered within the PSA are considered within the design basis assessment (e.g. spurious CMT actuation, spurious PRHR actuation, spurious CVS actuation, spurious CVS boron dilution, and consequential loss of off-site power). This latter list has been supplemented by the response to RO-AP1000-51 (Ref. 47) which has provided new ATWT analysis which includes analysis of the ATWT event following loss of off-site power.

89 Nevertheless, Westinghouse has acknowledged there is a need to review the PSA (Refs 19 and 38) list of faults for electrical system faults, support system faults, and C&I

initiating faults. Completion of these items has been raised by the PSA lead assessor as Assessment Finding **AF-AP1000-PSA-13** (Ref. 19). Clearly, following on from this work there is a need to consider whether any of these initiating events needs to be included within the design basis list. For this reason, Assessment Finding **AF-AP1000-FS-06** has been raised requesting a future licensee to review the findings of the response to **AF-AP1000-PSA-13** (Ref. 19) to see whether any of the new initiating events identified need to be considered within the design basis.

90 With regard to the issue of C&I initiating faults, during GDA Step 4 Westinghouse were requested under RO-AP1000-82 (Ref. 10) to review the consequences of spurious PMS actuation of any of the engineered safety features. This request was supplemented by additional requests TQ-AP1000-1175 and TQ-AP1000-1289 (Ref. 9). The aim was to see whether a diverse means of protection existed beyond the PMS to protect against faults initiated by the PMS. The focus being events such as spurious ADS actuation and spurious draining of the IRWST with the reactor still at power. These spurious initiating events are discussed in greater detail in Section 4.2.10 below.

4.2 Fault Sequences

91 SAP FA.3 requires that fault sequences should be developed from the initiating faults and their potential consequences analysed. SAP FA.4 requires that design basis analysis should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures. In order to assess whether these objectives have been achieved it is necessary to review each fault category on an individual basis. In the following sub-sections, the design basis analyses performed by Westinghouse will be reviewed in turn for each of the following fault categories:

- reactor trip faults;
- increase in heat removal from the primary system;
- decrease in heat removal by the secondary system;
- electrical supply faults;
- decrease in RCS flow rate;
- reactivity and power distribution anomalies;
- increase in reactor coolant inventory;
- decrease in reactor coolant inventory;
  a) Steam Generator Tube Rupture (SGTR);
  b) Small Break Loss of Coolant Accident (SBLOCA);
  c) Large Break Loss of Coolant Accident (LBLOCA);
- support system faults (including loss of cooling chain);
- control and protection system faults;
- spent fuel pool faults;
- shutdown faults;
- internal hazards, and;
- external hazards.

4.2.1 Reactor Trip Faults

4.2.1.1 Summary of Westinghouse's Safety Case

92 Faults in this category result in the spurious (or inadvertent) tripping of the reactor while it is operating normally at power. The possible causes of such a fault are failures of sufficient numbers of sensors measuring a single parameter in such a way as to cause a spurious reactor trip, failure within the protection system in such a way as to cause a reactor trip, or an operator manually tripping the reactor. This fault is the most frequent of the initiating faults that require a successful reactor trip and it therefore imposes the greatest reliability demands on the safety systems of the reactor.

93 The basis of the Westinghouse safety case is that a spurious reactor trip is a less severe transient than any other Condition II transient and so can be bounded by the turbine trip fault (Ref. 37) which results in a consequential reactor trip. This fault is included in the list of decrease in heat removal faults, which are discussed further in Section 4.2.3 below.

4.2.1.2 Assessment

94 While it is accepted that from a transient analysis perspective this fault can bounded by other more onerous transients, I have concerns about the long term control of reactivity aspects of this fault given its high initiating frequency. This is because following every reactor trip there will be an eventual reduction in the shutdown margin of the reactor core due to the decay of xenon. While the CMT and the IRWST systems provide diverse sources of borated water should the operator fail to ensure adequate shutdown margin using CVS as claimed in TQ-AP1000-1170 (Ref. 9), both these systems are also dependent upon operator action for actuation providing the Main Feedwater (MFW) or Start-up Feedwater system (SFW) operate as intended following reactor trip. Although the timescales are long (many hours) this implies a combined human reliability claim on the operator action of 1×10^{-7} per demand to meet the design basis target. It also potentially contradicts Westinghouse's claim that for every design basis fault on the AP1000 there is an automatic Class A1 system to mitigate the fault without the need for operator action for 72 hours. In the case of Sizewell B, there is an automatic actuation of the Chemical and Volume Control System (CVCS) following every reactor trip and the Emergency Charging System (ECS) is automatically actuated following failure of the CVCS to protect against this possibility. For this reason, Action 6 has been raised as part of the GDA Issue on diversity, under **GI-AP1000-FS-03**, requesting Westinghouse to consider the feasibility of automating the operation of the CVS following reactor trip and for the CMTs to be automatically actuated following failure of the CVS. Alternatively, Westinghouse will need to provide a consequence argument should the operator fail to ensure an adequate shutdown margin

4.2.1.3 Findings

95 As Action 6 of the GDA Issue on diversity, **GI-AP1000-FS-03**, Westinghouse is required to review the issue of diversity for long term reactivity control. Westinghouse is to consider the feasibility of automating the operation of the CVS following every reactor trip and to provide a consequence argument should the operator fail to ensure an adequate shutdown margin.

4.2.2 Increase in Heat Removal Faults

4.2.2.1 Summary of Westinghouse's Safety Case

96 Faults in this category result in a cool-down of the primary circuit. Given the negative moderator temperature coefficient of a PWR such faults result in an increase in the reactivity and power of the core potentially threatening the integrity of the fuel cladding should a Departure from Nucleate Boiling (DNB) occur. If a reactor is initially in the hot zero power condition, it may return to power as a result of the positive reactivity feedback induced by the cool-down, with a resultant increase in fuel temperature. Such faults can subject the RPV to a high-pressure low-temperature condition and a high rate of temperature reduction transient. If the fault is associated with a break in the secondary circuit, the fault may also lead to pressure and temperature loads which approach the design limits for the containment. There is also the potential for these faults to cause consequential SGTRs. Finally, a break in the secondary circuit outside containment has the potential for the largest release of radioactive material from design basis faults in this cool-down category.

97 The basis of Westinghouse's safety case is that it has reviewed a number of postulated events that it considers to be within the design basis of the plant and that could result in an increase in heat removal. For those cases which Westinghouse considers to be limiting, it has performed detailed analyses and demonstrated that even for the most bounding faults, the reactor protection system is able to trip the reactor, isolate the steam generators to reduce the rate of reactor cool-down, initiate post-trip cooling using the PRHR heat exchanger and initiate the flow of borated water from the CMTs to ensure an adequate shutdown margin.

98 In performing the transient analysis, Westinghouse assumes that the Rod Cluster Control Assembly (RCCA) with the highest worth fails to enter the core. Sensitivity studies have been performed on the effects of the unavailability of off-site power following reactor trip (which depending on what is assumed about the availability of off-site power determines whether the Reactor Coolant Pumps (RCP) may or may not trip), and on the size of the moderator reactivity feedback coefficient. Westinghouse also claims to have modelled the worst single failure in the reactor engineered safety features, which is that one of the discharge valves on the CMT fails to open. On the basis of the analysis presented, Westinghouse has concluded that adequate protection from DNB is provided for all the faults considered.

4.2.2.2 Assessment Overview

99 Westinghouse has considered the following faults within this category that it considers to be limiting and which are presented within the EDCD:

- feedwater system malfunctions causing a reduction in feedwater temperature;
- feedwater system malfunctions causing an increase in feedwater flow;
- excessive increase in secondary steam flow;
- inadvertent opening of a steam generator relief or safety valve;
- steam system piping failure, and;
- inadvertent operation of the PRHR heat exchanger.

100 All these events are considered to be Condition II events within Westinghouse's fault categorisation scheme, apart from the steam system piping failure which straddles the Condition III and IV boundary depending upon the size of the piping break.

101 I have chosen to sample the last four faults listed above on the grounds that steam system piping failure is the most limiting fault according to Westinghouse, while the excessive increase in secondary steam flow fault and the inadvertent opening of a relief or safety valve fault are judged to be the most bounding of the more frequent faults, and inadvertent operation of the PRHR is a fault that is unique to the AP1000.

102 In the sections below, I have separately presented my assessment of the limiting steam system piping failure from my assessment of the two bounding frequent faults and the inadvertent operation of the PRHR. I have also commented on Westinghouse's safety case for consequential SGTR failures following such faults, achieving safe shutdown and the assessment of radiological consequences from increase in heat removal faults.

103 Note that an assessment of the thermal hydraulic response of the containment vessel to these faults, which Westinghouse has presented in Chapter 6 of the EDCD, has been made but it is reported separately (Ref. 18).

4.2.2.3 Assessment of Steam System Piping Failure (Limiting Infrequent Fault)

Fault Sequence Analysis

104 The analysis of steam system piping failure assumes the rupture of a main steam line. In its response to RO-AP1000-46 (Ref. 37), Westinghouse states that the initiating frequency assumed for this event is 5.03×10^{-5} per year. For Sizewell B (Ref. 39) a main steam line rupture inside containment was assumed at a frequency of 1×10^{-4} per year while one outside containment was assumed at 1×10^{-3} per year. Such frequencies would appear to be consistent with the assumption of a Condition III / IV event being made by Westinghouse for AP1000. According to SAP FA.5, while such event frequencies can be considered infrequent, they are within the design basis and so it would be expected that the protection for such faults would meet the single failure criterion as required by SAPs FA.6, EDR.2 and EDR.4.

105 Westinghouse has treated the fault as a design basis event meeting the requirements of SAPs FA.4 and FA.5. The single failure it chooses to consider is a failure of a discharge valve on one of the CMTs. This is in addition to the assumption of the RCCA with the highest worth failing to enter the core. The assumption of a stuck RCCA is one of the standard deterministic assumptions made within the transient analysis studies of cooldown faults such as those considered here. It is a major factor in determining the shutdown margin of the reactor and whether the core returns to criticality following reactor trip. Making this assumption helps ensure that the overall assessment is conservative, consistent with the requirements of design basis analysis. The failure of a CMT discharge valve to open will reduce the rate at which borated water enters the core and so reduce the available shutdown margin at a given time in the transient. Therefore the claim that this is the bounding single failure appears plausible, especially given that the feedwater lines are provided with redundant isolation valves and the steam line break on the affected SG is not assumed to be isolated so bounding any single failure of a main steam isolating valve.

106 The protection signals are based upon 2-out-of-4 voting logic eliminating the possibility of a single failure. A unique feature of the AP1000 is that it automatically trips the RCPs following actuation of the 'S' safeguard signal so as to enable natural circulation flow from the CMTs into the reactor resulting in the injection of borated water. This has the additional advantage for cooldown faults that it reduces the rate of cooling from the affected SG that is depressurising. Failure to trip an RCP due to a single failure is avoided through the provision of redundant trip switchgear. Hence, I judge that the requirements of SAPs FA.6, EDR.2 and EDR.4 are met.

Methods and Assumptions

107 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling this fault sequence, Westinghouse has made the following assumptions to ensure a robust and conservative assessment:

- A bounding shutdown margin is used which assumes that the RCCA with the highest worth remains stuck out of the reactor following reactor trip. The calculation of shutdown margin is detailed in Chapter 4 of the EDCD (Ref. 16) for the first core and includes a number of allowances for calculational uncertainty. This analysis demonstrates that the assumed shutdown margin of 1600 pcm is bounding. The calculation assumes hot zero-power conditions but with equilibrium xenon conditions.
- An End of Cycle (EOC) moderator density coefficient is used for which the boron concentration is assumed to be zero, making the moderator coefficient most negative. This is a conservative assumption for cooldown transients.
- No decay heat is modelled to maximise the cooldown rate prior to return to criticality.
- The flow from the MFW and SFW systems is generally maximised in a bounding way to enhance the rate of cooldown from the steam generators. In addition, the PMS set-points for actuating reactor trip and for safeguard actuation and delay times on safeguard actuation signals include conservative allowances for errors and uncertainties.
- The modelling of steam flow through the break assumes perfect moisture separation within the SG resulting in a discharge quality of 1.0, which maximises the cooling efficiency of the SG as it depressurises.
- Manual actuation of the PRHR at time zero is conservatively assumed to maximise the cooldown.

108 These assumptions represent a standard approach to the design basis analysis of such faults and are comparable to those applied in the Sizewell B analysis. In particular, the assumptions of the double-ended guillotine break, the worst stuck RCCA, the conservative assessment of shutdown margin, the assumption of hot zero-power conditions, the maximum negative moderator coefficient, and the assumption of zero water entrainment through the SG break are judged to provide a bounding assessment meeting the requirements of SAP FA.7 (providing the analysis methods have been adequately validated).

109 The Westinghouse analysis uses the LOFTRAN computer code (Refs 40 to 42) to model the system transient. The analysis methodology that has been developed by Westinghouse for the steamline break assessment of passive plants requires that the point-kinetics model within LOFTRAN is switched off and that the reactivity data is instead provided in the form of look-up tables of core reactivity and power as a function of key core parameters. These tables are generated by fitting polynomials to a series of 3D steady-state reactor physics calculations (Ref. 41) performed using the ANC and THINC-IV computer codes coupled together. ANC is the reactor physics code while THINC-IV is a sub-channel thermal hydraulic code. The VIPRE-01 (Ref. 43) and FACTRAN (Ref. 44) computer codes are then used to determine whether DNB occurs. VIPRE-01 is also a sub-channel code while FACTRAN calculates the transient temperature profile within a fuel rod.

110 Given the importance of this calculational route, I decided in my GDA Step 3 report (Ref. 6) that there was a need to sample the validation of the LOFTRAN, ANC, THINC-IV

and VIPRE-01 computer codes. For this reason, the validation evidence for these codes has been assessed during GDA Step 4 against a relevant selection of the assurance of validity SAPs FA.17 to FA.22. In the case of the ANC and VIPRE-01 codes, the assessment of their validation is reported in the fuel and core assessment report (Ref. 17). This concludes that ANC is a suitable tool for core design while the analysis methods used in VIPRE-01 for the prediction of critical heat flux are satisfactory. The general validation of the LOFTRAN code is reported in Section 4.3.4 below although this is supplemented by additional comments specifically related to the validation of steamline break fault analysis (Refs 40 to 42) in the following paragraphs together with an assessment of the THINC-IV validation (Ref. 45) for this particular application.

111 The LOFTRAN and THINC-IV validation for steamline break analysis needs to cover a number of important phenomenon of which I have chosen to sample the following:

- the cool-down rate generated by the blowdown of one or more SGs due to a break in the secondary system;
- the mixing of buoyancy driven flows in the lower plenum and reactor core as a result of the highly asymmetric cooling conditions, and;
- the effect of buoyancy dominated flow on the coupling of thermal hydraulic and power distribution calculations for a core in conditions close to saturation.

112 Westinghouse has validated the LOFTRAN code for the SG break flow and secondary side conditions encountered in a steamline break fault through the SPES-2 tests (Ref. 42) as part of the original validation programme for the AP600 (i.e. an older reactor design that preceded the AP1000). The SPES-2 test facility is a full height, high pressure scaled facility that represents the reactor vessel, loops, pressuriser, steam generators, PRHR heat exchanger and the CMTs of the passive plant designs. A single blind test (Test 12) was performed representing a main steamline double-ended pipe rupture for conditions representative of hot-standby conditions.

113 The test measured pressuriser pressure, SG pressure, primary temperature, RCS flow, CMT flow and level and PRHR flow. The test was aimed at modelling RCS cooldown rate and did not model core decay heat or any core reactivity feedback effects. The report presents pre-test (blind) LOFTRAN predictions as well as post-test predictions against the experimental results. The pre-test base case calculation was performed with the standard design basis assumption of perfect moisture separation within the steam generator resulting in a discharge quality of 1.0 discussed above and assuming no line resistance. Although these factors contribute to the over prediction of the system cooldown, these modelling assumptions are used in LOFTRAN since they are conservative for design basis calculations. Following the tests, additional sensitivity studies were performed with LOFTRAN to demonstrate the adequacy of the model to represent key phenomenon. Sensitivities were performed on break flow quality and the mass of the SG structures to increase their thermal capacity. The report concludes that in each case, the code predicted the overall trends very well and the conservative nature of the break flow model in LOFTRAN was apparent. It also noted that the PRHR flow was well predicted and that the CMT was not seen to drain in either the test or the code predictions.

114 Having studied the results, I agree with Westinghouse's conclusions. The general trends are reproduced well. In the base case, the primary pressure falls much more quickly in the LOFTRAN prediction while the SG pressure falls at roughly twice the rate of the test results. In my view the results are a robust demonstration of the adequacy of LOFTRAN to conservatively model these transients, thereby meeting the requirements of SAP FA.7

and the assurance of validity SAP FA.18 which requires comparison of analytical models against appropriate experiments or tests.

115 In the case of coolant mixing in the lower plenum, Westinghouse makes the simple bounding assumption that the core inlet temperature is the minimum of the two inlet temperatures from the two loops (Ref. 41). This is clearly a conservative assumption as it maximises the reactor cooldown and so it is judged to meet the requirements of SAP FA.7.

116 On the AP1000, the RCPs are automatically tripped by the PMS following a steamline break fault and so the core flow is governed by buoyancy dominated natural circulation flow conditions (Ref. 41). In such circumstances, the loss of forced reactor coolant flow coupled with the assumption that the RCCA with the highest worth remains stuck out of the core following reactor trip produces highly skewed power gradients that result in significant cross-flow from the low-power regions of the core to the higher power regions near the stuck RCCA. Simple point kinetic assumptions are clearly inappropriate. It was for this reason that Westinghouse has developed a new methodology for calculating core reactivity and power on the AP1000, moving away from the approach that it uses for operating PWR plants which are assessed at full RCS flow. The lookup tables used instead of the internal LOFTRAN point-kinetics model take the form of two polynomials that are a function of key core parameters. These polynomial functions are generated by fitting the results of a series of steady state 3D coupled reactor physics and thermal hydraulic calculations performed using the ANC reactor physics computer code and the THINC-IV sub-channel code in which these key core parameters are varied.

117 I have two main observations about this approach. The first is that the reactivity and power polynomial functions were generated for an AP600 core design. The report covering the calculation (Ref. 41) argues that the shutdown margin for the AP1000 is expected to be greater than the AP600 although this is not obvious from the number of RCCAs on the AP600 (45) compared with the number on the AP1000 (53) given the increased size of the core. The report (Ref. 41) notes that the design basis Technical Specification limit for minimum shutdown margin assumed in the LOFTRAN code remains unchanged between the two designs at 1600 pcm. To achieve this shutdown margin, the worth of the RCCAs had to be adjusted to correct for the fact that the AP600 used a no-load temperature of 285°C compared with a no-load temperature of 291°C for the AP1000. In general then, there is a need to confirm that the core reactivity data assumed in the steamline break analysis is still consistent with the current AP1000 core design both for the first fuel cycle and also for future core reloads. For this reason, Assessment Finding **AF-AP1000-FS-07** has been raised for a future licensee to confirm that the proposed future core designs are consistent with the assumptions made in the steamline break analysis. Action 2 of GDA Issue **GI-AP1000-FS-02 i**s also related to this as it requires a consistent set of reactor core limiting conditions of operation (LCOs) to be developed as part of the GDA reference point design for AP1000.

118 The second point is that a steady-state reactor physics calculation is being used to perform the analysis and so the calculational route is incapable of representing any kinetic effects caused by the presence of delayed neutrons. As will be seen later from some GRS confirmatory analysis, such effects can be important in the initial phase of the return to power transient for these faults. It is therefore not clear that the steady-state approximation that Westinghouse is making is conservative when modelling these faults. With modern coupled code calculational techniques, it is now possible to develop models that can represent such effects. For this reason, Assessment Finding **AF-AP1000-FS-08** has been raised requiring a future licensee to demonstrate that the current approach is

conservative or to perform some coupled code analysis to confirm the conclusions of the Westinghouse analysis.

119 The validation of the THINC-IV sub-channel code for this application has been reviewed. The validation consists of a test performed at the Battelle-Pacific Northwest Laboratory (Ref. 45) with a rod bundle containing 12 electrically heated rods. The 12 rods were divided into two groups of 6, each forming a 2 x 3 array that were connected to different power supplies. In this manner, radial power distributions of interest were established for which detailed velocity and temperature profiles were measured at various axial locations. The test results are compared with predictions from THINC-IV and COBRA-IV sub-channel codes and are shown to be in good agreement. However, no discussion is given about the applicability of the test data to conditions in the reactor. In particular, no information is provided on absolute flow velocities and power ratings so it is difficult to judge how relevant the results are when scaled to fault conditions in a reactor.

120 Given the above discussion, Assessment Finding **AF-AP1000-FS-09** has been raised requiring a future licensee to review the validation evidence applied by Westinghouse to the steamline break methodology for buoyancy dominated flow conditions and to either demonstrate the adequacy of the evidence or to perform additional testing to improve the validation evidence.

Transient Analysis

121 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. In practice, for faults considered in this section, the aim of Westinghouse is to demonstrate this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB. To confirm that this objective has been achieved, the results of Westinghouse's design basis analyses need to be assessed.

122 The results of the Westinghouse transient analyses are summarised in Figures 15.1.5-2 and 15.1.5-7 of the EDCD which presents the return to power transient and core flow transient as a function of time respectively. The power peaks at about 220 seconds at about 4% of full power when the core flow is about 8% of nominal. However, the flux peaking factor associated with the worst RCCA being stuck out is not given. The results can be compared with the Sizewell B analyses (Ref. 39) which predicts a 14% peak return to power and a minimum DNBR[1] of 2.27. These results are not necessarily surprising since there are two significant differences in the approach adopted on the AP1000 design for dealing with cooldown faults when compared with Sizewell B. The first is that the RCPs on the AP1000 are automatically tripped on the low steamline pressure signal very early in the transient. This is done to permit the injection of borated water from the CMTs. This is not necessary on Sizewell B which relies upon the pumped High Head Safety Injection (HHSI) system to inject borated water. Tripping the RCPs also significantly reduces the rate of cooldown from the affected SG and so reduces the peak return to power. The second feature is that the AP1000 possesses a larger shutdown margin than Sizewell B. Although the AP1000 reactor core is smaller than the Sizewell B core, it contains the same number of shutdown RCCAs. For Sizewell B, the minimum

[1] To demonstrate that there is a margin to DNB, the standard approach is to calculate the maximum heat flux for the most limiting fuel assembly and compare the value with the critical heat flux (CHF) for those conditions at which DNB is predicted to occur, generating a DNB ratio (DNBR).

EOC shutdown margin with the worst RCCA stuck in its fully withdrawn position is 1.3 Niles (Ref. 39) while the design basis minimum shutdown limit for AP1000 from Table 4.3-3 of the EDCD is 1600 pcm (1.6 Niles) and so the lower return to power on the AP1000 is to be expected. However, it must be remembered that minimum DNBR is the appropriate safety limit for these faults rather than peak return to power.

123 Westinghouse has not presented the minimum DNBR results for the steam line break case in the EDCD, merely stating that it meets the design basis limit when judged against the W-3 Critical Heat Flux (CHF) correlation (Ref. 16). Westinghouse has chosen the DNBR design basis limit for the low pressures associated with cool-down faults which is low compared with the value of 2.0 that is assumed at Sizewell B (Ref. 46). Sizewell B uses the Groeneveld correlation for assessing DNB at low pressure. The value of 2.0 is chosen to give sufficient margin to cover the statistical uncertainties that apply to the critical heat flux correlations at the relevant conditions of low pressure and high quality.

124 The assessment of Westinghouse's W-3 CHF correlation is reported in the fuel and core design assessment report (Ref. 17). This concludes that the uncertainty allowance included in the design basis limit may be too low given that the primary pressure during a steamline break fault typically reduces to about 38 bar and that in any case the validation documentation is not satisfactory for use in a safety case. For this reason, the Fuel and Core topic area assessment report (Ref. 17) has raised an Assessment Finding, **AF-AP1000-FD-10**, requiring the future operator to provide suitable documentation justifying the use of the W-3 or a suitable alternative correlation for the pressure, flow and quality regimes associated with steamline break faults.

Confirmatory Analysis

125 GRS has repeated the steamline break analysis from hot zero power using its own ATHLET systems code coupled together with its own 3D QUABOX/CUBBOX reactor kinetics code. The results of its comparison (Ref. 25) show good agreement with Westinghouse predictions on both the primary and secondary side. As noted above, the Westinghouse modelling of steam flow through the break assumes perfect moisture separation within the SG, resulting in a discharge quality on 1.0. GRS has used a homogeneous equilibrium model to represent the flow through the flow limiter. This results in the entrainment of water through the break. This is to be expected given that water will be flashed off in the affected SG as it depressurises. This means that the results of the GRS analysis will be slightly more realistic (contains less conservatism) than the Westinghouse results. Despite the differences in break modelling, the predictions of fall off in SG pressure (in the SGs that depressurise) are very similar in the two sets of analyses. On the primary side, the temperatures at the inlet and outlet of the CMT on the SG loop associated with the blowdown, and at the inlet and outlet of the PRHR are similar although the Westinghouse analysis predicts a slightly greater cooldown (to be expected given the differences in the break flow modelling). On the primary side, the prediction of boron injection from the CMTs is very similar (an important parameter for these reactivity insertion transients).

126 The agreement of the transients in terms of changes in reactivity and power levels is less good. The predictions of the initial reactivity transients are in good agreement, suggesting the moderator temperature coefficients are very similar. However, once the cores return to criticality the transient predictions are seen to diverge. The GRS analysis predicts a continuing reactivity increase until prompt criticality is approached at about 700 pcm. The rapid increase in core power and the associated feedback effect causes the transient to

turn over and return to a level which just about remains critical. The power level is seen to reach an approximate steady-state at about 4%.

127 In contrast, the Westinghouse calculation predicts a slower return to power once the core returns to criticality. However, it continues to rise and does not appear to approach prompt criticality condition despite the fact that the reactivity transient is seen to exceed 1900 pcm. In my judgement, this feature is probably an artefact of the Westinghouse analysis methodology in which reactivity is determined from a steady-state calculation. It is noticeable that once the transients settle out at a steady-state condition the predictions converge with the Westinghouse power level prediction at about 3% which is comparable but slightly less than the GRS prediction of 4%.

128 In my opinion, the comparable steady-state power levels are reassuring and suggest that the strategy of tripping the RCPs and limiting the cooldown rate does significantly reduce the predicted return to power compared with conventional PWRs. Nevertheless, there are some question marks about the validity of the Westinghouse methodology which supports the need for Assessment Finding **AF-AP1000-FS-08** discussed above requiring a future licensee to demonstrate that the fault analysis of the main steamline break fault from zero power is conservative or perform analysis using a coupled code analysis. Nevertheless, given the conservatisms made in the bounding assumptions discussed above, I am generally satisfied with the provision of protection on the AP1000 for this fault and judge that the requirements of SAP FA.7 have been met.

Sensitivity to Xenon Level

129 The analysis reported in the EDCD (Ref. 16) assumes equilibrium xenon conditions. It is accepted that the choice of hot zero power is bounding for the double-ended guillotine break of a main steamline in terms of the resultant peak return to power following reactor trip. However, the choice of hot zero power is made to cover the full reactor operating power range from 0% to 100% power and so in principle the xenon level can be at any intermediate range, potentially changing the shutdown margin available by about 3000 pcm. It was therefore initially unclear if the assumption of equilibrium xenon conditions was a bounding one.

130 For this reason, TQ-AP1000-836 (Ref. 9) was raised, requesting Westinghouse to perform a sensitivity study on the effects of the initial xenon concentration. In its response, Westinghouse argues that the operator would increase the boron concentration to maintain adequate shutdown margin against the Technical Specification limit and that this would have the benefit of reducing the moderator temperature coefficient from that assumed in the zero boron reference case presented in the EDCD. While this argument is accepted, it ignores the possibility of a steamline break occurring when the reactor is returning to power following shutdown operations when both xenon level and boron concentration could be low. However, in these circumstances, it is judged unreasonable to request Westinghouse to consider as a credible design basis fault sequence a cooldown fault occurring on a reactor at hot standby conditions with zero xenon and boron concentrations and a RCCA stuck out of the core. Without the presence of a stuck RCCA, the reduced flux peaking factors would probably ensure there is an adequate margin to DNB but this will need to be confirmed. For this reason, Assessment Finding, **AF-AP1000-FS-11** has been raised, requiring a future licensee to review the case of steamline break occurring at hot zero power conditions with zero xenon and boron concentrations but with all rods inserted.

Sensitivity to Break Size and Power Level

131 In my Step 3 report, I noted that no sensitivity studies to break size and power level are presented within the EDCD. In contrast, such parametric sensitivity studies were presented for Sizewell B (Ref. 39). Given that the size of the Sizewell B integral flow restrictors on the steam generators is identical to those on the AP1000 at 0.13 m^2, I judge that these results will give an indication of the sensitivity to these parameters for the AP1000. The Sizewell B report demonstrates that for larger breach sizes starting the transient calculation from the hot zero power condition is bounding in terms of the minimum DNBR with tripping provided on low steam line pressure. For smaller break sizes, including stuck open safety or relief valves, operation at full power is more bounding in terms of the minimum DNBR. In such cases, tripping is provided by overpower trips based upon neutron flux measurements. I noted that these results appear to contradict the Westinghouse analyses, which assume that starting at zero power is bounding for both the main steam line break fault and the stuck open relief or safety valve fault. For this reason, TQ-AP1000-836 (Ref. 9) was raised, requesting Westinghouse to produce further sensitivity studies to break size and power level to confirm the conclusions of their analysis during GDA Step 4. The response confirms that for intermediate break sizes, the full power case is more bounding than the zero power case in terms of DNBR because the low steamline pressure trip is largely ineffective and so the pre-trip transient is prolonged. The analysis reported is for standard Westinghouse plant and not for AP1000. In particular, the sensitivity studies to breach size at full power do not consider the implications for two loop plant and do not consider the higher power densities and the increased SG size that apply to the AP1000 design. In my judgement the response is insufficient and for this reason, as part of Action 2 of GDA Issue **GI-AP1000-FS-03**, Westinghouse is being requested to perform this explicit analysis for the AP1000 design for a reactor at full power.

132 It is noticeable that the Westinghouse analysis is claiming the ex-core detectors to perform the neutron flux measurements to trip the reactor. These detectors were not claimed in the Sizewell B safety case (Ref. 39) because of concerns over the calibration of the detectors due to the reduction in the temperature of the water in the down-comer that occurs during a cool down fault. From discussions, it is understood that Westinghouse claim the digital Protection and Monitoring System (PMS) monitors the cool leg temperatures and can correct for this effect. A study of Chapter 7 of the EDCD confirms that the T_{cold} temperature is input into the PMS overpower and over-temperature trip channels but the determination of the correction algorithm has not been assessed during GDA Step 4. Westinghouse will need to provide information on how this algorithm has been derived as part of the justification made in response to Action 2 of GDA Issue **GI-AP1000-FS-03** discussed above.

4.2.2.4 Assessment of Excessive Increase in Secondary Steam Flow [including Inadvertent Opening of a Steam Generator Relief of Safety Valve] (Limiting Frequent Fault)

Fault Sequence Analysis

133 Westinghouse concedes that the excessive increase in secondary steam flow and inadvertent opening of a steam generator relief or safety valve are Condition II events. As such, these are frequent events and so Westinghouse has reviewed these faults in its responses to RO-AP1000-47 (Ref. 29) and RO-AP1000-51 (Ref. 47). In its response to RO-AP1000-47 (Ref. 29), Westinghouse has identified three limiting fault sequences that need to be assessed to demonstrate that the AP1000 has diverse means of achieving each safety function for these faults:

- Excessive increase in steam flow with failure of RCCAs to insert;
- Excessive increase in steam flow with failure of PMS, and;
- Excessive increase in steam flow with failure of CMT injection.

134 Note that in the above list and the following discussion, the excessive increase in steam flow event should also be taken to include (bound) the inadvertent opening of either a SG Power Operated Relief Valve (PORV) or a SG Main Steam Safety Valve (MSSV) fault. The first two sequences result in ATWT events[1] while the third prevents the rapid injection of borated water once the reactor has been tripped. In my opinion, the above list misses three additional fault sequences that also need to be discussed:

- Excessive increase in steam flow with failure of RCP trip;
- Excessive increase in steam flow with failure of feedwater isolation, and;
- Excessive increase in steam flow with failure of main steamline isolation.

135 The first increases the rate of cooldown post-trip and prevents the CMTs from injecting borated water in the primary circuit while the last two increase the post-trip rate of cooldown. Westinghouse has bounded the other safety functions and potential fault sequences by the loss of normal feedwater fault which is discussed in Section 4.2.3 below. It should be noted that of the above six sequences; the last four sequences are concerned with short term reactivity control during the post-trip transient. In these cases the inadvertent opening of a relief or safety valve while at hot zero power will be the bounding initiating event because these valves are not isolated following reactor trip. Each of these six sequences is discussed in the following sub-sections.

Excessive Increase in Steam Flow with Failure of RCCAs to Insert

136 Westinghouse supplied some preliminary ATWT analysis (Refs 63 to 65) during GDA Step 3. However, the analysis started from the position that the loss of feed fault with failure to trip was the bounding fault due to concerns over primary circuit integrity. This ignored faults such as excessive increase in steam flow where the safety limit of concern is DNB. For this reason, RO-AP1000-51 was raised requiring Westinghouse to present analysis considering a failure to successfully shutdown the reactor during events such as an excessive increase in steam flow fault.

137 The particular sequence under consideration here is an excessive increase in steam flow fault in which the RCCAs are assumed to fail to insert due to a mechanical common mode failure resulting in an ATWT event. Although Westinghouse has discussed this event in sub-section 7.1.3 of its response to RO-AP1000-51 (Ref. 47), it only considers increases in secondary steam flows that are less than 10% of normal flow, stating that flow increases that are greater than this requiring the reactor to trip are presented in sub-section 7.1.4 of its response to RO-AP1000-51 (Ref. 47) covering inadvertent opening of a steam generator relief or safety valve. However, in that sub-section, it is stated that inadvertent opening of a relief or safety valve will not result in a reactor trip. The report

[1] Protection against all the limiting design basis faults requires the initiation of a reactor shutdown so that the reactor power is rapidly reduced so easing control of the transient. Many design basis faults can be expected to occur relatively frequently with initiating event frequencies greater than 1×10^{-3} per year. Such faults are therefore known as frequent faults or in the case of very frequent faults, anticipated transients. Where such a fault occurs without reactor trip, it is described as an Anticipated Transient without Trip (ATWT).

therefore fails to provide discussion of excessive increases in steam flow which require a reactor trip.

138 As noted above, Westinghouse has not performed a sensitivity study for secondary break sizes at full power and so Action 2 of GDA Issue **GI-AP1000-FS-03** has been placed for such analysis to be performed. Excessive increases in steam flow and inadvertent opening of relief or safety valves at full power have similar effects to a break on the secondary side and so also need to be considered under Action 2 of **GI-AP1000-FS-03**, both for the successful reactor trip case and for the ATWT sequence discussed here in order to demonstrate adequate primary and diverse protection.

Excessive Increase in Steam Flow with Failure of PMS

139 This sequence also results in an ATWT event but this time the common mode failure that prevents the reactor shutting down is associated with the PMS failing to initiate the reactor trip signal. For the excessive increase in steam flow and intermediate secondary side break faults being considered here, the most effective protection is likely to be flux instrumentation and yet the DAS is not provided with any flux protection. For this reason, Westinghouse not only needs to demonstrate adequate protection for this fault under Action 2 of **GI-AP1000-FS-03** but, in addition, Westinghouse needs to consider the feasibility of connecting the in-core detectors to a suitably diverse protection system such as the Class A2 DAS or the Class A2 portion of the PLS to provide a diverse means of flux protection to the ex-core flux detectors. This issue has been raised as Action 2 under **GI-AP1000-FS-04**.

Excessive Increase in Steam Flow with Failure of CMT Injection

140 This sequence is concerned with failure of the CMT to inject. For these faults, short-term reactivity control is normally aided by the injection of borated water from the CMTs. In its response to RO-AP1000-47 (Ref. 29), Westinghouse does not present any transient analysis for this sequence effectively arguing that this safety function is bounded by the need for long-term reactivity control following the decay of xenon, which is explicitly considered for the case of loss of normal feedwater fault (discussed in Section 4.2.3 below). However, Figure 15.1.4-2 of the EDCD (Ref. 16) demonstrates that even with successful CMT injection there is a slight return to power following the inadvertent opening of a relief or safety valve case and so there is a need to consider short-term reactivity control for these faults.

141 However, in practice, my judgement is that this sequence can be bounded by the following sequence in which the failure to trip the RCPs results in an additional cooldown as well as the consequential failure of the CMTs to inject.

Excessive Increase in Steam Flow with Failure of RCP Trip

142 This sequence assumes the failure of the RCPs to trip. As noted above, such a failure will not only result in a faster cooldown transient but will also prevent the injection of borated water from the CMTs. In such circumstances, the return to power will inevitably be greater than that presented in Figure 15.1.4-2 of the EDCD, although it should be noted that there is a significant safety margin in the base case presented in the EDCD and the larger flow associated with the operation of the RCPs will mitigate to some extent the effects of the increased return to power with regard to DNB. Nevertheless, in my opinion this is the bounding fault for the short-term post-trip control of reactivity safety function

and so it is important that the safety case presents an analysis of the fault to confirm there are adequate safety margins to appropriately justified criteria subject to ALARP. For this reason, Assessment Finding **AF-AP1000-FS-12** has been raised requesting a future licensee to provide such an assessment.

Excessive Increase in Steam Flow with Failure of Feedwater Isolation

143 This sequence assumes failure to isolate the feedwater system due to a common mode failure of the isolation valves. This has the potential to increase the cooldown experienced by the reactor by providing additional water into the SG that is under going the blowdown. It may well be that a diverse means exists to automatically isolate the feedwater system on the AP1000 either through the use of a diverse set of isolation valves or through tripping the main feedwater pumps but such means have not been identified in the response to RO-AP1000-47 (Ref. 29). Alternatively, given the size of the safety margin in the base case, it may be that failure to isolate the feedwater system might have acceptable consequences. Assessment Finding **AF-AP1000-FS-13** has been raised for a future licensee to confirm the basis of the safety case.

Excessive Increase in Steam Flow with Failure of Main Steamline Isolation

144 This sequence assumes failure to isolate the main steam system due to a common mode failure of the main steam isolating valves. This has the potential to increase the cooldown experienced by the reactor as both SGs can continue to depressurise through a common steam header. As with the previous sequence, it may well be that given the size of the safety margin in the base case, failure to isolate the steam system might have acceptable consequences but this needs to be demonstrated. Assessment Finding **AF-AP1000-FS-14** has been raised for a future licensee to confirm the basis of the safety case.

Sensitivity to Two Stuck RCCAs

145 In my GDA Step 3 report, I noted that the Sizewell B analysis (Ref. 39) performs sensitivity studies to the case of two stuck RCCAs for the more frequent cool-down faults on the basis that the conditional probability for this event could not be excluded from the design basis sequence requirement of 1×10^{-7} per year (Ref. 7). For this reason, TQ-AP1000-836 (Ref. 9) requested Westinghouse to perform a sensitivity study for two stuck RCCAs.

146 In its response, Westinghouse argues that it is unlikely that the two RCCAs with the highest worth would be adjacent to each other and so the power shape is unlikely to be much worse than the single stuck RCCA case and therefore given the low return to power and the large margins to DNB, Westinghouse concluded that additional analysis was not necessary. However, Westinghouse is assuming that the importances of adjacent RCCAs do not interact significantly and that the additional stuck RCCA will not change the shutdown margin significantly so that the return to power will not be very different. In my judgement, this needs to be further demonstrated and so I have raised Assessment Finding **AF-AP1000-FS-15** for a future licensee to demonstrate that adequate margins to DNB remain following any two RCCAs remaining stuck out of the core.

4.2.2.5 Assessment of Inadvertent Operation of the PRHR Heat Exchanger

Fault Sequence Analysis

147 Spurious initiation of the PRHR heat exchanger is a fault that is unique to the AP1000 since no other civil PWR design contains such a design feature. Westinghouse has correctly identified that this initiating event has the potential to cause a cooldown that needs to be considered within the design basis analysis, in accordance with the requirements of SAPs FA.4 and FA.5. Westinghouse argues that there is no limiting single failure that needs to be considered other than the failure of one of the redundant trains (called a protection division) of the PMS and that this does not have any effect on the transient analysis presented. I accept this argument and so I judge that the requirements of SAP FA.6 have also been met.

148 In its response to RO-AP1000-46 (Ref. 37), Westinghouse states that the initiating frequency assumed for this event is between 1×10^{-1} and 1×10^{-2} per year. As such this is a frequent fault and Westinghouse has analysed the fault in its responses to RO-AP1000-47 (Ref. 29) and RO-AP1000-51 (Ref. 47). It should be noted that during GDA Step 4, Westinghouse have introduced a design modification to the PMS to trip the reactor following spurious opening of one of PRHR discharge valves (Ref. 48). The motivation for the design change is to prevent PCI failures occurring to the fuel as a result of this transient, but it obviously has an added advantage in terms of providing an additional means of protection against DNB. Nevertheless, the need for diversity requires failure of the PMS to be considered. To this end, Westinghouse has presented analysis of this fault sequence in its response to RO-AP1000-51 (Ref. 47).

Methods and Assumptions

149 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling this fault sequence, Westinghouse have made the following assumptions to ensure a robust and conservative assessment:

- An EOC moderator coefficient value is used (conservative for cooldown transients).
- No credit is taken for the heat capacity of the reactor coolant system and the SG metal in attenuating the resulting plant cooldown.
- Reactor trips on high neutron flux, over-temperature and overpower ΔT trips are ignored consistent with an ATWT analysis.

150 These assumptions are judged to provide a bounding assessment meeting the requirements of SAP FA.7.

151 The Westinghouse analysis uses the LOFTRAN computer code (Refs 40 to 42) to model the system transient while the VIPRE-01 (Ref. 43) and FACTRAN (Ref. 44) computer codes are then used to determine whether DNB occurs. VIPRE-01 is a sub-channel code while FACTRAN calculates the transient temperature profile within a fuel rod. As noted in Section 4.2.2.3 above, the assessment of the validation evidence of the VIPRE-01 code is reported in the fuel and core assessment report (Ref. 17). The general validation of the LOFTRAN code is reported in Section 4.3.4 below with additional comments specifically related to the modelling of the PRHR heat exchanger in Sections 4.3.1 to 4.3.3. In summary, the methods are judged to meet the requirements of the validity of assurance SAPs FA.17 to FA.24 and SAP FA.7.

Transient Analysis

152 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. In practice, for the inadvertent operation of the PRHR fault considered in this section, the aim of Westinghouse is to demonstrate that this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB. I have assessed the results of Westinghouse's design basis analysis to reach a view on whether this objective has been met.

153 The results of the Westinghouse transient analysis studies are summarised in Figures 7.1-9 to 7.1-12 of its response to RO-AP1000-51 (Ref. 47). Following inadvertent initiation of the PRHR, the core power is seen to increase to about 119% power from full power (assuming manual control of the RCCAs) before stabilising at 110% power as illustrated in Fig 7.1-9 of the response to RO-AP1000-51 (Ref. 47). Figure 15.1.6-6 of the EDCD (Ref. 16) also shows that for the virtually identical transient conditions, the minimum DNBR will be about 1.9 with the transient pressure remaining comfortably within the range of validity of the WRM-2M CHF correlation. In my opinion, based upon the analysis presented by Westinghouse, the requirements of SAP FA.7 have been met for this fault.

154 It should be noted that this transient effectively places a sizing restriction on the PRHR in that it provides a design limit on the maximum heat removal capability of the system. The sizing of the PRHR is therefore a compromise between minimising the heat removal capability to reduce the rate of cool-down for this fault and the requirements for other faults, such as the loss of feed faults and SGTR faults, where the need is to maximise the heat removal capability.

Confirmatory Analysis

155 GRS who performed the steamline break analysis has also repeated the inadvertent operation of the PRHR fault analysis at full power using its own ATHLET systems code and its own 3D QUABOX/CUBBOX reactor kinetics code coupled together. The results of its comparison (Ref. 25) show good agreement with Westinghouse's predictions on both the secondary and primary side. In particular, the agreement of the transients in terms of changes in reactivity and power levels is good. The Westinghouse calculation predicts a larger increase in power compared with the GRS results because it models a greater heat removal capability than GRS for the PRHR. This is because Westinghouse deliberately biases its design basis calculations to be conservative by adjusting the PRHR heat transfer coefficients and flow resistance data within LOFTRAN code depending upon whether the minimum or maximum heat removal rate is conservative for a given application (Ref. 49). In contrast, the GRS analysis is performing an essentially best estimate calculation. Despite these differences, I consider that the GRS analysis to be completely supportive of the Westinghouse analysis and confirms that the requirements of FA.7 have been met.

4.2.2.6 Consequential Failures

156 No discussion is presented within the steamline break analyses about the possibility of consequential SGTR failures as a result of the transient. This is perhaps appropriate given this design transient section is attempting to demonstrate adequate shutdown margin to protect against DNB. Nevertheless, it is understood that for Sizewell B the conditional failure frequency for consequential SGTR is assumed to be as high as

1×10^{-1} per demand. If such high frequencies are reflected within the AP1000 design, there is a case for considering such sequences to be within the design basis according to SAP FA.5. For this reason, TQ-AP1000-838 (Ref. 9) was raised requesting Westinghouse to provide additional arguments or analysis to justify its position.

157 In its response to the TQ, Westinghouse has assessed the consequences of three possible fault sequences covering consequential SGTR. The first fault sequence considers a main steamline break inside containment in coincidence with a consequential SGTR. This fault is not limiting since the release from the SGTR is to containment such that the fault is bounded by spurious ADS sequences.

158 The second fault sequence considers a main steamline break occurring downstream of the MSIV. The depressurisation of the secondary side is assumed to cause a single SGTR. The secondary side depressurisation transient results in the PMS isolating the MSIV and so the fault effectively transforms into a standard SGTR fault but with an immediate automatic reactor trip. Given that the fault does not assume any additional single failures such as failure of the MSIV to close on demand it is argued that the radiological consequences will be bounded by the normal SGTR fault sequence.

159 The third fault sequence also considers a main steamline break occurring down stream of the MSIV but assumes that the MSIV fails to close. Given Westinghouse's own PSA gives a sequence frequency of 5×10^{-5} per year ($5 \times 10^{-4} \times 0.1$) for the previous fault sequence, the additional single failure needs to be considered as a potential design basis sequence unless it can be bounded by another design basis fault. Since the affected SG is not immediately isolated, Westinghouse state that the ADS will be actuated depressurising the RCS and terminating the break flow either automatically or by operator action after 30 minutes. Westinghouse claims that on the basis that no fuel damage will occur, the fault is very similar to the failure of small lines carrying primary coolant outside containment analysed within the EDCD. As noted in Section 4.2.2.4 above, Westinghouse will need to demonstrate that no fuel failure occurs for the excessive increase in steam flow case under Action 2 of **GI-AP1000-FS-03** to confirm this claim. This claim also possibly ignores the fact that more than one consequential SGTR failure could occur as a result of the initial transient, although given the sequence frequency this may not be so important since Westinghouse argue that the radiological consequences from the failure of the small lines LOCA case are bounded by an order of magnitude by the 10 mSv release from the double ended cold leg guillotine break LOCA. Given the frequency of the sequence of 1×10^{-7} per year ($5 \times 10^{-5} \times 2 \times 10^{-3}$), providing the requirements of Action 2 of **GI-AP1000-FS-03** are met, I am content with these arguments which comfortably meet the Basic Safety Level (BSL) requirements of SAPs Target 4 and Target 8.

4.2.2.7 Controlled State to Safe Shutdown State

160 In my GDA Step 3 report, I noted that there was no discussion on how the reactor will be brought from the controlled state to the safe-shutdown state within the EDCD analysis. For this reason, RO-AP1000-52 (Ref. 10) was raised for Westinghouse to extend the safety case for each design basis fault to the safe shutdown state. In its response to RO-AP1000-52 (Ref. 35), Westinghouse divides its response into three common groupings of faults: intact circuit faults, LOCA faults, and SGTR faults. Increase in heat removal faults fall into the intact circuit fault grouping.

161 As intact circuit faults include both frequent and infrequent faults, Westinghouse identifies both a primary and diverse means of achieving the safe shutdown state for the four safety functions reactivity control, decay heat removal, reactor inventory control and reactor

pressure control using only passive Class A1 systems (with the exception of the DAS). The primary means relies upon CMT injection for reactivity control and inventory control, the PRHR cooled by the IRWST and the PCS for decay heat removal with automatic actuations provided by the PMS. The diverse means relies upon manual bleed and feed[1] using the ADS, accumulators and IRWST injection for reactivity and inventory control and short-term decay heat removal and sump recirculation with cooling from the PCS for long-term decay heat removal. Manual control is provided though the DAS. Note that both the primary and diverse means of achieving the decay heat removal safety function require the IRWST and PCS systems. However, Westinghouse identifies that the active Class A2 systems can provide an additional diverse means of achieving these functions including the decay heat removal function. These other means use the CVS for reactivity and inventory control, the SFW system for providing cooling to the SGs to provide short-term decay heat removal and the RNS cooled by the CCS and Service Water System (SWS) for long-term decay heat removal. The control function is provided by the PLS and operator action.

162 The Westinghouse response is not detailed enough for specific faults to provide an adequate final safety case. In particular, it does not identify any fault specific operator actions required for individual faults such as the increase in heat removal faults. For example, in the case of faults involving breaks on the secondary side, operator recovery actions might be needed to ensure the isolation of the affected SG, to prevent a further cooldown, to maintain a low containment pressure, to conserve water in the SFW storage tank and to limit potential flooding. The operator might also be needed to supply feed to the remaining SG from the SFW system while the CVS or CMT might be needed to increase the boron concentration in the primary circuit to maintain an adequate shutdown margin. There might also be a need to re-align feedwater supplies from the affected SG to the intact SG. For this reason, Assessment Finding **AF-AP1000-FS-16** has been raised for a future licensee to provide a safety case covering the transition from controlled state to shutdown state for each specific fault with a view to preparing the post-accident recovery procedures.

4.2.2.8 Radiological Consequence Assessment

163 SAPs FA.3 and FA.7 require that radiological consequence analysis, on a conservative basis, should be performed for each design basis fault sequence that can lead to the release of radioactive material. Within GDA Step 3, no attempt was made to review the radiological consequences analysis supporting the design basis assessment for these faults since it was known that the Westinghouse analysis had been made against US criteria. For this reason RO-AP1000-48 was raised requesting Westinghouse to analyse the radiological consequences of design basis faults against the UK requirements given in SAPs FA.3, FA.7 and Target 4.

164 A detailed review of the radiological consequence analysis methodology applied by Westinghouse in its response to RO-AP1000-48 is presented in Section 4.6 below. The conclusion of this review is that in general the radiological consequences methodology appears sensible and conservative but that in some areas further justification will be required as part of site licensing process. On this basis, it is my judgement that the methodology presented in the RO-AP1000-48 response (Ref. 50) is broadly appropriate for this preliminary GDA Step 4 assessment of individual faults against Target 4 in the HSE SAPs.

[1] The term bleed and feed refers to the operator action of manually depressurising the RCS by opening the ADS valves which allows the safety injection systems to inject coolant directly into the RCS to remove decay heat from the core.

165 The response to RO-AP1000-48 (Ref. 50) argues that the consequences of an excessive increase in secondary steam flow fault and the spurious opening or failure to close of a safety relief valve fault can be bounded by the release from the loss of off-site power fault. This is also a Condition II event. Westinghouse argues that this sequence is bounding even though the SG relief valves are assumed to operate normally because a stuck open relief valve on the AP1000 plant results in the affected SG being isolated. In contrast, if the safety relief valves operate normally, they continue to open and close for an extended period. This claim has not been assessed during Step 4 but can be reviewed as part of the closure of Action 1 of GDA Issue **GI-AP1000-FS-02**. The predicted radiological release from the loss of off-site power fault is 0.05 mSv which comfortably meets the BSL limit of Target 4.

166 Westinghouse has performed a radiological assessment for the main steamline break fault (Ref. 119). The estimated release is 5.6 mSv which given the assumed frequency of 5×10^{-5} per year meets the Target 4 BSL limit of 100 mSv.

4.2.2.9 Findings

167 Following my assessment of increase in heat removal faults, I am broadly content with the fundamental design of the AP1000 to protect against this class of fault. I judged that significant protection is provided for these faults by the large shutdown margin on the AP1000, the strategy to trip RCPs and rapidly inject borated water from the CMTs, and the ability to isolate both SGs and rely solely upon the PRHR to remove decay heat. I also welcome the decision by Westinghouse to provide an extra trip signal to protect against inadvertent actuation of the PRHR.

168 I have a remaining concern on the adequacy of the protection system to protect against those faults that result in intermediate cooldown rates with the reactor at full power. The adequacy of the protection system to trip the reactor sufficiently quickly to avoid DNB has not been demonstrated. These faults are potentially frequent and so this concern has implications for the requirements of both the primary and diverse protection systems. For this reason, Action 2 has been raised under the GDA Issue on diversity, **GI-AP1000-FS-03**, to review the protection provided for these faults. A related issue has been raised as Action 2 of **GI-AP1000-FS-04**, in which Westinghouse is to consider the feasibility of connecting the in-core detectors to the DAS to see if these could provide a diverse and automatic means of flux protection.

169 In addition, a number of assessment findings have been raised. In general, these are items requiring further analysis or additional validation evidence rather than a fundamental issue with the design and in my judgement they can be closed out as part of the site licensing process.

4.2.3 Decrease in Heat Removal Faults

4.2.3.1 Summary of Westinghouse's Safety Case

170 The maintenance of design conditions in the reactor depends, among other things, on preserving (within limits) the continuity of heat flow from the reactor through the primary and the secondary cooling systems to the turbines. Faults in this group result in an imbalance of the heat flow so that the heat produced in the reactor is not matched by the capacity of the remainder of the system to remove it. These faults lead to a heat-up of the primary circuit with the potential to challenge the integrity of the fuel cladding and cause the primary pressure to rise challenging the integrity of the primary circuit. Following successful reactor trip, it is necessary to ensure that adequate post-trip cooling is

provided to avoid flooding the pressuriser. Failure to do so will seriously challenge the integrity of the primary circuit. For a given size of pressuriser, faults in this category, together with the increase in reactor coolant inventory faults and the SGTR faults discussed below, effectively determine the minimum heat removal requirements for the PRHR heat exchanger and also limit the maximum size of the CMTs. They also place the greatest demands on the reliability of primary and secondary circuit over-pressure protection. If the fault is associated with a feed line break in the secondary circuit, the fault may also lead to pressure and temperature loads on the containment although these are generally less onerous than those from a steam line break. Given the high pressures possible in the primary and secondary circuits, there is the possibility that safety relief valves will lift on either or both circuits and then for these to consequentially fail to reseat. Failure of a relief valve on the primary side to reseat will result in a consequential LOCA.

171 The basis of Westinghouse's safety case is that it has reviewed a number of postulated events that it considers to be within the design basis of the plant and that could result in a decrease in heat removal. For those cases which Westinghouse considers to be limiting, it has performed detailed analyses and demonstrated that even for the most bounding faults, the PMS is able to trip the reactor and initiate adequate post-trip cooling using the PRHR heat exchanger.

172 In performing the transient analysis, Westinghouse has performed sensitivity studies on the effects of the availability of offsite power following reactor trip, which, depending on the assumption made, can result in the tripping of the RCPs. It also claims to have modelled the worst single failure in the reactor engineered safety features, which is that one of the discharge valves on the PRHR fails to open. On the basis of the analysis presented, Westinghouse has concluded that the PRHR provides adequate levels of post-trip cooling for all the range of faults considered, such that the pressuriser never becomes water solid; threatening the structural integrity of the primary circuit.

4.2.3.2 Assessment Overview

173 Westinghouse has considered the following faults within this category that it considers to be limiting and which are presented within the EDCD:

- steam pressure regulator malfunction or failure that results in decreasing steam flow;
- loss of external electrical load;
- turbine trip;
- inadvertent closure of main steam isolation valves;
- loss of condenser vacuum and other events resulting in turbine trip;
- loss of ac power to the station auxiliaries;
- loss of normal feedwater flow, and;
- feedwater system pipe break.

174 All the above events are considered to be Condition II events, with the exception of a feedwater system pipe break, which Westinghouse consider to be a Condition IV event. I have chosen to sample three of the faults listed above; the feedwater system piping failure (this is the most limiting fault according to Westinghouse), loss of normal feedwater flow (the most bounding of the more frequent faults in terms of the performance of the PRHR), and inadvertent closure of the MSIVs (the most bounding fault of the more frequent faults in terms of overpressure protection).

175 My assessment of the three sampled faults is presented separately in the sections below. I have also commented on Westinghouse's safety case for consequential failures, achieving safe shutdown and the assessed radiological consequences from decrease in heat removal faults.

4.2.3.3 Assessment of Feedwater System Pipe Break Fault (Limiting Infrequent Fault)

Fault Sequence Analysis

176 The feedwater system piping failure assessment assumes the rupture of a main feed line. In its response to RO-AP1000-46 (Ref. 37), Westinghouse claims that the initiating frequency for this Condition IV design basis event is 4×10^{-4} per year. This frequency appears to be reasonable given that a pipe break is a passive failure. According to SAP FA.5, such event frequencies, while they can be considered infrequent, are within the design basis and so it would be expected that the protection for such faults would meet the single failure criterion as required by SAPs FA.6, EDR.2 and EDR.4.

177 Westinghouse has indeed treated the fault as within the design basis, meeting the requirements of SAPs FA.4 and FA.5 and has identified what it considers the most onerous single failure (failure of one discharge valve on the PRHR). The failure of a PRHR discharge valve to open will reduce the rate that the PRHR is able to remove decay heat from the primary circuit such that the claim that this is the bounding single failure appears plausible given that the protection signals that are claimed are all based upon 2-out-of-4 voting logic. However, the Westinghouse analysis predicts that the PSVs lift and there is no discussion about the implications of one of these failing to reseat on demand (as the assumed single failure). During GDA Step 4, Westinghouse has provided arguments that this possibility is bounded by the Condition II inadvertent opening of a pressuriser safety valve case. These arguments are discussed further below in the section on consequential failures (Section 4.2.3.6).

178 The assumption made about whether a consequential loss of grid occurs as a result of the reactor trip normally needs careful consideration for transients involving loss of feed. This is because loss of grid results in the RCPs coasting down. When operating, the RCPs contribute extra heating that is comparable to the level of decay heating. On the other hand, tripping the RCPs results in a reliance on natural circulation cooling which causes a reduction in the removal of heat from the core by the SGs (and the PRHR in the case of AP1000) and thus an increase in the average core temperature. Comparison of the loss of ac power to the station auxiliaries fault which results in both loss of feed and consequential RCP tripping and the loss of normal feedwater fault (analysed in Sections 15.2.6 and 15.2.7 of the EDCD respectively) shows that the extra heating from the RCPs is the dominant effect. However, for the feedline break fault, the effect will be much less significant because the SG blowdown causes the RCPs to be tripped[1] on the low steamline pressure signal only five seconds after the reactor trip signal is received.

179 The design of the PRHR system warrants discussion under the single failure criterion requirements defined in SAPs FA.6, EDR.2 and EDR.4 since it is a safety system that consists of only a single cooling train. With the exception of the PRHR discharge valves, which are provided with redundancy and for which the EDCD claims there will be regular testing, there are two normally open non-redundant valves. Westinghouse argues that all of the non-redundant valves on the PRHR system will be left in the open position during

[1] The RCPs are tripped deliberately in order to enable the CMTs to inject borated water.

normal operation and that failure of these non-redundant valves in the closed position represents a passive failure and is highly unlikely. However, there is no way of directly testing whether the non-redundant valves are in the correct position once the reactor is at power since end to end testing, as recommended by SAP EMT.7, will only be possible on the PRHR during outages. There are alarms on the position indicators to eliminate human errors but these will not be able to detect un-revealed passive single failures with the valves themselves, which does not meet the recommendations of SAP ESS.5.

180 In considering whether the PRHR system meets the single failure criterion, it should be remembered that the single failure criterion defined in SAP EDR.4 applies only to the safety function and not to a safety system. In its response to RO-AP1000-47 on passive single failures (Ref. 32), Westinghouse argues that the PRHR meets the single failure criterion since the safety function to which it is contributing is the removal of decay heat and there is a diverse means of achieving the safety function by actuating the ADS allowing cooling from the PXS. In its response, Westinghouse also states that actuating the SFW would provide a diverse means of cooling although I note that this is not the case for the feedline break fault as the feed to the SGs is taken from a common header. The claim on feed and bleed using the ADS system is judged to meet the requirements of the SAPs EDR.2 and EDR.4 subject to evidence being provided to validate these claims. However, the responses to RO-AP1000-47 (Refs 29 and 32) only demonstrate the diverse bleed and feed capability for the loss of normal feedwater fault. No demonstration is provided for the feedline break fault which is a more onerous fault since only one of the SGs retains water and so the ability to remove decay heat by discharging steam through the PORVs is reduced. In my judgement, the difference in the conditions of the SGs is unlikely to invalidate the claim on bleed and feed. However, I have raised Assessment Finding **AF-AP1000-FS-17** for a future licensee to provide transient analysis to confirm that this is the case.

181 An obvious way to protect against a single failure would be to provide a second PRHR. However, it should be recognised that a passive piping failure on the PRHR resulting in a loss of coolant fault would not be protected against by the addition of another PRHR train. This is because the PRHR is only qualified for operation when the pressure of the primary circuit is above the discharge pressure of the accumulators due to concerns associated with the injection of nitrogen (i.e. it is not claimed for LOCA faults, which is what a piping failure on the PRHR would be). In addition, as Westinghouse notes in its response to RO-AP1000-47 (Ref. 32), it is highly undesirable to introduce a second 100% PRHR heat exchanger system because of concerns over spurious operation of both PRHRs at the same time. As discussed in the previous section, Westinghouse's own analysis demonstrates that the inadvertent operation of just one PRHR is sufficient to raise reactor power by 20% while providing two 50% PRHRs would reduce the reliability of the system to achieve its safety function of removing decay heat since both systems would need to operate. Finally, it should be noted that Sizewell B is not able to meet the single failure criterion for the feedline break fault without claiming bleed and feed since the four SG feedlines are paired together such that the feedline break results in the loss of feed to two SGs. With preventative maintenance and a single failure the safety function cannot be achieved so there is already a precedent. In my opinion, based upon the above discussion, and subject to satisfactory resolution of Assessment Finding **AF-AP1000-FS-17**, I accept that the provision of a single PRHR is adequate and that the single failure requirements of SAPs FA.6, EDR.2 and EDR.4 have been met.

Methods and Assumptions

182 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling this fault sequence, Westinghouse has made the following assumptions to ensure a robust and conservative assessment:

- At the start of the transient, interaction between the break and the feedline and the main feedwater control system is assumed to result in a complete loss of feedwater flow to both steam generators. No feedwater is delivered to, or lost through the steam generator nozzles.
- No credit is taken for the high pressuriser pressure trip, over-temperature ΔT trip, high pressuriser level trip or high containment pressure trip. Instead, the reactor trip signal is assumed to be initiated when the low SG narrow-range level set-point is reached on the ruptured steam generator.
- After reactor trip, the faulty SG is assumed to blow down through a double-ended break area of 0.16 m^2. A saturated liquid discharge is assumed until all the water inventory is discharged from the faulted steam generator. This minimises the heat removal capability of the faulted steam generator and maximises the resultant heat-up of the reactor coolant. No feedwater flow is assumed to be delivered to the intact steam generator.
- The plant is assumed to be initially operating at 102% power. Conservative core residual heat generation is assumed based upon long-term operation at the initial power level preceding the trip. The initial reactor coolant average temperature is conservatively assumed to be 3.61°C above the nominal value while the pressuriser pressure is conservatively assumed to be 3.45 bar below the nominal value. The initial pressuriser level is conservatively set at a maximum value while a conservative initial SG water level is assumed in both SGs.
- No credit is taken for charging or letdown.
- Pressuriser safety valve set-point is assumed to be at its minimum value.
- The PRHR heat exchanger is actuated by the low SG water narrow range level (in coincidence with low SFW flow) signal. A 15-second delay is assumed following the low level signal to allow time for the alignment of the PRHR heat exchanger valves.
- SG heat transfer area is assumed to decrease as the shell-side liquid inventory decreases. The heat transfer remains at approximately 100% in the faulted SG until the liquid mass reaches about 11%. From that point, the heat transfer is assumed to reduce to 0% as the liquid inventory reduces to zero.

183 These assumptions represent a standard approach to the design basis analysis for such faults and (apart from the unique aspects introduced by the PRHR) are comparable to those applied in the Sizewell B analysis. In particular, the assumptions with regard to break flow modelling and tripping on low SG level are judged to provide a bounding assessment since studies performed by Westinghouse (Ref. 51) demonstrate that more realistic modelling of the double ended feedline break would result in an initial cooldown of the reactor.

184 The Westinghouse analysis uses the LOFTRAN computer code to model these heat-up transients. I am aware that the LOFTRAN code has been modified to incorporate modelling of the passive features on AP1000 such as the PRHR heat exchanger and the CMTs which operate under natural circulation conditions. For this reason, the validation of LOFTRAN has been reviewed during GDA Step 4 and this is reported in Section 4.3 below as part of the assessment of the passive safety systems for non-LOCA faults. This

assessment identifies the need for a future licensee to analyse the results of commissioning tests that Westinghouse is proposing will be performed during the hot functional testing and power ascension on the first AP1000 plant to be built, and to confirm that the performance of the PRHR and the IRWST is consistent with the claims in the safety case. These requirements are respectively covered by Assessment Findings **AF-AP1000-FS-18** and **AF-AP1000-FS-19.** The review in Section 4.3 concludes that subject to satisfactory confirmation from the first of a kind commissioning tests, the validation evidence for the LOFTRAN modelling of the PRHR is sufficient to meet the requirements of SAP FA.7.

Transient Analysis

185 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. In practice, for the faults considered in this section, the aim of Westinghouse is to demonstrate this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB, that adequate decay heat removal is achieved, and that the primary and secondary pressure limits are not exceeded. I have assessed the results of Westinghouse's design basis analysis to reach a view on whether this objective has been met.

186 In Fig 15.2.8-5 of the EDCD (Ref. 16), the LOFTRAN modelling of the pressuriser pressure transient is presented for the feedline break fault. The pressure transient is seen to be doubly humped. The initial peak is due to the loss of feed caused by the feedline break reducing the amount of heat taken out by the SGs. This causes the primary circuit to heat-up until the reactor is tripped on low SG water level. The peak pressure is sufficient to cause the pressuriser safety relief valves to open. Following reactor trip, the primary circuit cools and the safety relief valves close. The remaining intact SG starts to dry out. This causes the second peak in the primary pressure as the circuit heats up again. The pressuriser safety relief valves re-open and the pressuriser level starts to rise as the water in the primary circuit expands as it heats up. The PRHR is then initiated on low narrow range SG water level in coincidence with low SFW flow.

187 The pressuriser water volume transient for the feedline break fault is presented in Fig 15.2.8-6 of the EDCD. The analysis demonstrates that the PRHR has sufficient heat removal capacity to prevent the pressuriser from becoming water solid and it is ultimately capable of cooling the primary circuit as the level of the decay heat reduces. Fig 15.2.8-6 suggests that there is little margin on the pressuriser water level and so it is important to have confidence in the LOFTRAN code for the estimating natural circulation flow and heat removal capacity of the PRHR. The validation of the LOFTRAN model for the PRHR is discussed in the previous section but it is also important that the performance of the IRWST and PCS which provide the cooling chain and ultimate heat sink functions for intact circuit faults are also validated. The assessment of the validation of the PCS is reported in the containment and severe accident report (Ref. 18) but this has been supplemented by additional comments specifically related to its role in cooling the IRWST during intact circuit faults in the following paragraphs.

188 Within the EDCD, there is no design basis assessment of the containment performance for these faults even though the PCS provides the ultimate heat sink for such faults once the PRHR causes the water in the IRWST to boil. The steam evaporated from the IRWST is cooled and re-condensed on the walls of the containment vessel, which is cooled by the PCS. The design intent is that the re-condensed water from the containment vessel is

collected in a condensate gutter at the operating deck level and re-cycled back into the IRWST. This appears to be a major omission in the documentation of the safety case since it is important to demonstrate that the passive containment cooling system is functionally capable of returning sufficient condensed water back to the IRWST for a period of 72 hours without operator action. In its responses to TQ-AP1000-296, TQ-AP1000-481 and TQ-AP1000-1023 (Ref. 9), Westinghouse has not provided a detailed technical justification for the assumed condensate return efficiency of 95%.

189 This high efficiency is crucial. Condensate water will form on components and structures in the containment and has the potential to drain some condensate directly into containment sump by-passing the IRWST. If not enough water is returned to the IRWST, there could be a consequential failure of the PRHR after a number of hours of boiling possibly requiring manual actuation of the ADS.

190 Westinghouse has performed a large scale integral test (Refs 59 and 60) to validate the thermal hydraulic codes used for modelling the response of the containment to LBLOCA and main steamline break faults. However, the AP1000 Phenomena Identification and Ranking Table (PIRT) and Scaling report (Ref. 53) acknowledges that the test was not well scaled for transient conditions since the rate of steam production was insufficient to match the transient conditions found in LBLOCA and main steamline break faults. Steaming due to IRWST boiling (as seen in the loss of feed faults) is a less demanding transient and so steady state conditions might be more representative. However, the scaling of the test also under represented the surface area of the heat sink structures in the containment by about an order of magnitude compared with the plant design. This is probably conservative for overpressure calculations as it minimises condensation but with regard to the current application, the reverse will be the case.

191 For these reasons, GDA Issue **GI-AP1000-FS-06** has been raised requiring Westinghouse to provide validation evidence that the IRWST is functionally capable of cooling the PRHR during intact circuit faults for 72 hours.

192 A related issue is the effect of containment pressure on the heat removal capacity of the PRHR. The increase in pressure associated with boiling in containment will raise the saturation temperature of the IRWST affecting its performance as the cooling system for the PRHR. Westinghouse identified that this effect was sufficient to reduce the margin to overfill for SGTR faults (Ref. 61), which has resulted in a design change (Ref. 62) to the set-point of the SG high-2 level isolation signal which isolates the CVS and SFW systems. As part of the above GDA Issue, **GI-AP1000-FS-06**, Westinghouse has therefore also been asked to review the effect of containment pressure on loss of feed faults where the concern is on the margin to overfill of the pressuriser.

4.2.3.4 Assessment of Inadvertent closure of both Main Steam Isolating Valves (Limiting Frequent Fault – Short-term Overpressure)

Fault Sequence Analysis

193 Westinghouse has classified the ‘inadvertent closure of both MSIVs fault’ as a Condition III event. In the EDCD, Westinghouse has chosen to bound the fault using the turbine trip transient, in which it is assumed that the MSIVs close at the same speed that the turbine-stop valves close. This combined bounding fault therefore places the greatest demands on the reliability of the primary and secondary overpressure protection.

194 As a Condition III event, it could be as frequent as 1×10^{-2} per year. The expectation for a fault of this frequency in the UK is that a diverse means of protection is provided for each

safety function. As a result, Westinghouse was requested to review this fault as part of its response to RO-AP1000-47 (Ref. 10) in order to demonstrate functional diversity.

195 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has identified the need to study the following fault sequence associated with turbine trip in which the effects of inadvertent closure of both MSIVs are included:

- Turbine trip (MSIV closure) with failure of the PSVs.

196 This fault sequence assumes the common mode failure of the PSVs to open on the primary side following turbine trip (including inadvertent closure of both MSIVs). In my opinion, there is also need to consider the following fault sequence:

- Turbine trip (MSIV closure) with failure of the MSSVs.

197 This second sequence is to cover the common mode failure of the MSSVs to open on the secondary side following turbine trip (including inadvertent closure of both MSIVs). The transient analysis presented in the EDCD for the turbine trip fault already covers the case for failure of the Power Operated Relief Valves (PORV) to open.

Turbine Trip (MSIV Closure) with Failure of the PSVs

198 The RCS overpressure protection safety case for the AP1000 design is presented in Chapter 5.2.2 of the EDCD rather than in Chapter 15 on fault analysis. On the AP1000, protection of the reactor pressure boundary against such overpressure faults is provided by two spring loaded PSVs. These are sized with the intention of providing protection against the following list of transients:

- loss of electrical load and/or turbine trip (including MSIV closure);
- uncontrolled RCCA withdrawal at power;
- loss of reactor coolant flow;
- loss of normal feedwater, and:
- loss of off-site power to the station auxiliaries.

199 The EDCD states that, in practice, the capacity of the relief valves to meet this requirement is based on analysis of a complete loss of steam flow to the turbine with the reactor continuing to operate at 102% power conditions. Feedwater is assumed to be lost and no credit is taken for operation of the pressuriser level control, the pressuriser spray, the RCCA control system, the steam dump or the steamline PORVs although the MSSVs are claimed. The reactor is assumed to remain at full power and not trip. The capacity of the PSVs is required to be as large as the maximum in surge rate into the pressuriser during the transient. Westinghouse claim that this practice results in a safety valve capacity well in excess of the capacity required to prevent the system exceeding the 110% RCS design pressure for the events listed above. Certainly, the pressure predictions calculated by LOFTRAN and presented for the turbine trip fault in Figure 15.2.3-16 of the EDCD, suggest that they are adequate to keep the pressure below the 110% limit. The minimum design flow for a PSV is quoted as 94.4 kg/s (340 te/hr) giving a total flow of 188.8 kg/s. This compares favourably with Sizewell B which has a capacity of 158.4 kg/s from its three PSRVs although this is supplemented by an additional 52.8 kg/s from the two POSRVs. After taking account of a single failure, the total PSV flow would be 94.4 kg/s on the AP1000. This is broadly comparable with a total POSRV flow on Sizewell B of 105.6 kg/s given that although the

reactor powers are identical for the two designs, the sizing of the pressurisers are significantly different.

200 The provision of only two PSVs contrasts with the position at Sizewell B which is provided with three spring loaded Pressuriser Safety Relief Valves (PSRV) as well as two diverse Pilot Operated Safety Relief Valves (POSRV). The lift pressure for the POSRVs is set below that for the PSRVs with the intention that any over pressure transient will preferentially result in the opening of the POSRVs. The greater relief capacity provided by the PSRVs is held in reserve for less frequent faults. This strategy recognises the higher consequential failure probability of the spring loaded valves failing to close as compared with the more complex, pilot-actuated POSRVs. It should be noted that the auxiliary feedwater system on Sizewell B is capable of providing sufficient feed to the steam generators to avoid the lifting of the PSRVs. In comparison with Sizewell B, the primary side of the AP1000 appears to have no diverse safety system to protect against the common mode failure of the PSVs. Westinghouse has addressed this issue in its response to RO-AP1000-47 (Ref. 29).

201 For the case of turbine trip covering inadvertent closure of all MSIVs with common mode failure of the PSVs, the closure of all the MSIVs causes an increase in the pressure of the secondary system. As a consequence, the heat removal capability is reduced and this causes the temperature and pressure of the primary system to also increase, culminating in a reactor trip on high hot leg temperature. However, the primary side PSVs are assumed to fail to open and the primary pressure reaches a peak pressure of 214.6 bara before the opening of the MSSVs on the secondary side starts to restore heat removal from the primary side. The analysis demonstrates that the peak pressure is below the primary pressure limit of 221.0 bara applicable for such low frequency events. No details of the assumptions made in the calculation are provided and so it is difficult to form a judgement about the adequacy of the calculations. While the results look plausible, given the small margins, it is necessary for a future licensee to provide further details on the assumptions and methods used in the calculation. For this reason, I have raised an Assessment Finding, **AF-AP1000-FS-20**, for this information to be provided.

Turbine Trip (MSIV Closure) with Failure of the MSSVs

202 The steam system overpressure protection safety case is presented in Chapter 10.3 of the EDCD. On the AP1000, protection against over-pressurisation of the secondary side is provided by one PORV and six MSSVs on each of the two SGs. The MSSVs are sized to provide sufficient capacity to prevent steam pressure exceeding 110% of the main steam design pressure during the following transients:

- turbine trip without reactor trip and with main feedwater maintained, and;
- turbine trip with a delayed reactor trip and with loss of main feedwater flow.

203 The minimum design flow for an individual MSSV is quoted as 172.6 kg/s at 110% SG pressure, giving a total flow of 1036 kg/s per SG which can be compared with the nominal feed flow of 943 kg/s. The PORV can provide a maximum additional flow of 128 kg/s although the design minimum at 110% pressure is not quoted in the EDCD. Hence the valve capacities are sufficient to cover nominal full steam flow conditions even with a single failure of one MSSV. The number and sizing of individual valves is chosen to limit the increase in secondary steam flow to less than 10% following spurious operation.

204 This situation can be compared with Sizewell B which is provided with one PORV and five MSSVs on each of its four SGs. The minimum design flow for an individual MSSV is

112 kg/s, giving a total flow of 560 kg/s per SG compared with the nominal feed flow of 477 kg/s. The PORV can provide an additional flow of 122 kg/s.

205 After making allowance for the additional number of SGs on the Sizewell B design, the valve capacities are seen to be broadly comparable given that the reactor powers are identical for the two designs and recognising that with just two SGs on the AP1000 design it is desirable to limit the individual valve capacities because of concerns over spurious operation as mentioned in Section 4.2.2.4 above. A noticeable exception is the PORV capacity which is almost identical for the two designs despite the differing number of SGs. On the AP1000, an individual PORV can only remove 13.6% of the reactor power. This will be more than adequate for long-term post-trip cooling but it is not clear whether the valve is functionally capable of providing a diverse means of pressure relief during the turbine trip transient with common mode failure of the MSSVs. While I recognise that the design pressure safety limit of 110% can probably be relaxed given the likely sequence frequency there is clearly a need for this transient to be analysed.

206 In summary, Westinghouse has not presented any analysis for the case of inadvertent closure of both MSIVs with common mode failure of the MSSVs in its response to RO-AP1000-47 (Ref. 29). For this reason, Assessment Finding **AF-AP1000-FS-21** has been raised, requesting a future licensee to provide such analysis to demonstrate the integrity of the pressure boundary of the main steam system.

4.2.3.5 Assessment of Loss of Normal Feedwater (Limiting Frequent Fault – Decay Removal and Long-Term Overpressure)

Fault Sequence Analysis

207 Westinghouse categorise the loss of normal feedwater as a Condition II event. As such, it is a frequent event which within the traditional UK approach to design basis analysis, requires two diverse safety systems to be provided for each safety function. In its response to RO-AP1000-47 (Ref. 29), Westinghouse has identified the following limiting fault sequences that need to be assessed to demonstrate that the AP1000 has diverse means of achieving each safety function:

- loss of normal feedwater with failure of RCCAs to insert;
- loss of normal feedwater with failure of PMS;
- loss of normal feedwater with failure of PRHR;
- loss of normal feedwater with failure of CMT injection;
- loss of normal feedwater with failure of PCS, and;
- loss of normal feedwater with failure of PSVs.

208 Westinghouse has bounded other fault sequences by the excessive increase in secondary steam flow fault in Section 4.2.2 above or the turbine trip fault (covering inadvertent MSIV closure) discussed in the previous section. My assessments of Westinghouse's transient analysis of these fault sequences, aimed at demonstrating the adequacy of the diverse safety systems to replace the failed "front-line" safety systems assumed to be unavailable for the normal feedwater fault are presented below.

Loss of Normal Feedwater with Failure of RCCAs to Insert

209 Loss of normal feedwater fault with failure of the RCCAs to insert results in the ATWT sequence that is the most onerous in terms of over-pressurisation of the RCS. In the case

of AP1000, loss of feed to the SGs results in the tripping of the RCPs, the actuation of the CMTs (which inject borated water into the core) and the actuation of the PRHR. Tripping the RCPs reduces the coolant density in the reactor core and enhances the negative moderator temperature coefficient. This strategy differs from that applied at Sizewell B, which is provided with a diverse emergency boration system to protect against ATWT faults. Westinghouse is claiming that the actuation of the CMTs together with tripping of the RCPs will provide adequate diverse protection for such faults given the inherent characteristics of the moderator temperature coefficients on PWRs. If justified, such a claim would meet the requirements of SAP ERC.2 which requires that there should be at least two diverse systems provided for shutting down a civil reactor.

210 In its response to RO-AP1000-47 and RO-AP1000-51 (Refs 29 and 47), Westinghouse has presented a revised set of ATWT analyses (Ref. 47). These analyses supersede some earlier ATWT analyses (Refs 63 to 65) performed prior to the implementation of tripping the RCPs and actuation of the CMTs by the DAS by the low wide range SG level signal and which only focused on the overpressure criteria.

211 The response to RO-AP1000-51 (Ref. 47) reviews the implications of ATWT events for the whole range of frequent faults in the decrease in heat removal fault class. The faults considered are loss of external load, turbine trip, inadvertent closure of MSIVs, loss of condenser vacuum, loss of ac to plant auxiliaries and loss of normal feedwater. It concludes that the loss of normal feedwater event is the most limiting fault in terms of peak over pressure, while the loss of ac to plant auxiliaries resulting in the RCPs tripping is covered by the loss of flow faults considered in Section 4.2.4 below.

212 Westinghouse has performed a largely best estimate analysis. The plant initial conditions reflect nominal full power values and no measurement or instrumentation errors are assumed. Nevertheless, the initial pressuriser level is assumed to be at the top of its control dead-band. Beginning of Cycle (BOC) reactivity coefficients corresponding to where the burnable poisons are depleted are assumed since this is known to give the most positive moderator coefficient and so will be the most onerous point of the fuel cycle for ATWT analysis. A conservative flow area is assumed for the PSVs and operation of the CVS letdown valves is not credited. Operation of the start-up feedwater system is also not credited. Finally, although the CMTs are part of the protection against this fault, Westinghouse state that their operation is not modelled in the transient analysis due to difficulties in modelling saturation conditions in the cold leg within the LOFTRAN code. The transient analysis does model the beneficial effect of the RCP trip. The identified design limits are to avoid pressurising the reactor vessel above 228 bara and preventing the fuel from entering DNB.

213 The analysis is performed with the LOFTRAN computer code using its point kinetics model, although the reactivity coefficients assumed in the analysis are cross-checked with a 3-D steady-state reactor physics calculation performed using the ANC computer code, the validation for which is reviewed in the fuel and core assessment report (Ref. 17). Westinghouse claim that this aspect of the methodology is conservative since the steady state calculation performed using ANC results in a power shape associated with maximum reactivity rather than the distorted power shape caused by delayed neutrons. Westinghouse claims that in reality the delayed neutrons will delay the change in power shape causing a lower reactivity and lower power. Given the complexity of this argument, I commissioned GRS to perform some confirmatory analysis using coupled 3D reactor kinetics and system codes. This work is reported in the next section.

214 The results presented for the fault (Figures 7.2-6 to 7.2-11, Ref. 47) show that as the SGs empty due to loss of feedwater, the pressure and the temperature of the RCS start to increase. After 47 seconds, a reactor trip signal is generated on low narrow range SG

level which causes the turbine to trip and the turbine bypass control is switched to pressure mode. However, the turbine bypass system is unable to remove all the heat and the SG PORVs and MSSVs open. The increase in temperature of the RCS causes the core power to reduce due to moderator feedback. The increasing pressure causes the PSVs to open at 58 seconds. The reduction in power continues until the core matches the energy removed by the SGs at 70% power. At this point, heat transfer through the SG tube bundle continues to degrade as the remaining liquid in the secondary side of the SGs is boiled off. This reduction in SG heat transfer causes temperatures to rise still further and core power to reduce due to moderator feedback. When the SG level reaches the low wide range SG level set-point at 67 seconds, PMS (or DAS) operates the PRHR (at 76 seconds) and DAS operates the CMTs (at 81 seconds) and trips the RCPs (at 74 seconds). Although the report states that the actuation of the CMTs is not modelled, the transient analysis shows that the boron concentration increases suggesting that the CMTs were modelled in the transient. The pressuriser becomes water solid at 83 seconds and the RCS reaches its peak pressure at 199 bara. The pressure then starts to fall as core power reduces because of the moderator feedback effect caused by the reduction in flow. Since the CMTs should borate the core, the reactor will become sub-critical with the PRHR removing decay heat.

215 The peak pressure is well below the structural integrity limit of 221 bara and suggests that adequate protection is provided for this fault sequence meeting the requirements of SAP FA.7 without the need for a fast acting Emergency Boration System (EBS) as provided at Sizewell B.

216 The moderator reactivity coefficients that Westinghouse has assumed in its ATWT analysis (Ref. 47) are not the same as those outlined in Chapter 4 of the EDCD (Ref. 16) and which were originally intended to form the basis of future LCO limits. In the UK, ATWT events are regarded as being within the design basis and therefore any assumptions with regard to moderator temperature coefficients made in the ATWT analysis needs to be captured within the Technical Specifications. As noted in Section 4.2.2.4 above, Action 2 of GDA Issue **GI-AP1000-FS-02** has been raised requiring Westinghouse to determine a consistent set of reactor core LCOs as part of the GDA reference point design for AP1000. In addition, to ensure that the assumptions made in the Westinghouse analysis remain valid for all future fuel cycle conditions including the initial core and so to ensure the requirements of SAP ERC.2 are achieved in practice, Action 1 of GDA Issue **GI-AP1000-FS-03** on functional diversity for frequent faults has been raised requiring Westinghouse to capture the assumed moderator reactivity coefficients within its Safety Analysis Checklist (Ref. 143).

Confirmatory Analysis

217 GRS has repeated (Refs 23 and 24) the loss of normal feedwater ATWT analysis performed by Westinghouse. A preliminary calculation (Ref. 23) was performed with ATHLET using a point kinetics model. A second calculation (Ref. 24) was performed using the ATHLET systems code coupled with the 3D QUABOX/CUBBOX reactor kinetics code (although the latter approach is shown to have little effect on the results). The results of the GRS comparisons (Refs 23 and 24) with the Westinghouse analysis (Ref. 47) generally show good agreement, although the GRS moderator coefficients are less conservative (i.e. a better estimate of moderator behaviour in reality).

218 The primary side and secondary side predictions are generally similar although the GRS analysis suggests that the initial equilibrium conditions where the secondary heat removal rate matches the primary power level occurs at a slightly lower power level. This is almost

certainly due to slight differences in the modelling of the effect of SG water level on primary to secondary heat transfer area. Heat removal by the PRHR is very similar in the two comparisons. The amount of boration from the CMTs varies significantly between the two analyses which is not unexpected given there is an uncertainty about how Westinghouse has modelled the CMTs in this transient. However, this only affects the long term shutdown margin and both analyses agree that the core remains significantly sub-critical. The peak pressure occurs earlier in the transient and so will not be affected by this difference. The primary flow rates are similar with the timing of RCP trip being within 4 seconds off each other in an 1800 second transient. Secondary pressures are identical. GRS initially predict lower primary pressures and temperatures than Westinghouse and consequently lower flows through the PSVs. This is almost certainly reflecting the better estimate moderator coefficients used in the GRS analysis.

219 The comparison has improved my confidence in the Westinghouse analysis methodology using LOFTRAN. In my judgement, the requirements of SAP FA.7 have been met. In particular, it has confirmed my view that there is no need to require Westinghouse to install a fast acting emergency boration system on the AP1000 on the basis of this comparison. I therefore judge that the response (Ref. 47) has met the requirements of RO-AP1000-51.

Loss of Normal Feedwater with Failure of PMS

220 The case of loss of normal feedwater with failure of PMS to trip the reactor is discussed in Westinghouse's response to RO-AP1000-51 (Ref. 47). This argues that the DAS is fully capable of protecting against this fault since it can trip the reactor on low SG wide range level and initiate the PRHR, CMTs and the PCS and trip the RCPs to provide both the decay heat removal and long-term reactivity control functions. No transient analysis is presented for this case. Presumably, this is because Westinghouse judges that the transient is effectively bounded by the previous transient (failure of the RCCAs to insert) since the DAS is available to drop the RCCAs into the core rapidly reducing reactor power and pressure. However, the initial transient up until the time of reactor trip will be slightly more onerous as the DAS set-point is on the low SG wide range level while the PMS trip set-point is on low SG narrow range level and this will delay the time until turbine trip occurs in the previous transient. This transient is worth studying to see if the DAS is functionally capable of preventing the pressuriser from going water solid since this increases the conditional probability of the PSV failing to reseat (it will lift during the transient) resulting in a consequential LOCA. For this reason, I have raised Assessment Finding **AF-AP1000-FS-22** for a future licensee to perform this analysis to confirm that the choice of the DAS low SG wide range set-point is ALARP.

Loss of Normal Feedwater with Failure of PRHR

221 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has identified manual bleed and feed (which in this sub-section will be called Sequence 1) using the ADS and IRWST injection systems as a diverse Class A1 passive means of providing the decay heat removal function. It has also identified the active Class A2 SFW system (which in this subsection will be called Sequence 2) as a diverse "other" means of providing this function.

222 From a systems perspective, it is interesting to compare the provision of diversity on the AP1000 with that on Sizewell B. Sizewell B is provided with three diverse feed systems; the redundant motor driven feed to the SGs, redundant steam turbine driven feed to the

SGs, and bleed and feed using the safety injection system which is provided with redundancy but requires manual operation. The AP1000 is claiming three diverse heat removal systems; the active Class A2 start-up feedwater system which provides feed to the two SGs, natural circulation cooling using the single passive Class A1 PRHR system, and cooling using the passive Class A1 ADS and PXS systems which are provided with redundancy. There is potentially a fourth using the Class A2 RNS but discussion of that system will be presented under SBLOCA faults in Section 4.2.8.5 below.

223 Most safety systems on Sizewell B are also provided with four-fold redundancy. The design basis assumption (Ref. 31) is that one of the four trains will fail as a consequence of the initiating fault, a second train will be lost as a consequence of the single failure criterion, and the third train is assumed to be out for maintenance. Hence, it is the fourth train that provides the required safety function. Clearly, if on-load preventative maintenance on a safety system is forbidden by the Technical Specifications, as is the case for the AP1000 passive safety systems, and extra diversity is provided, then the requirement for a safety system to have four redundant trains can begin to be relaxed. Westinghouse is effectively claiming that the safety function for removing decay heat from the reactor primary circuit when the reactor is still pressurised is provided by three trains of cooling, the two SGs with start-up feedwater, and the one PRHR. In my judgement, this meets the single failure requirements of SAPs FA.6, EDR.2 and EDR.4 and possibly exceeds them given that one of the trains (the PRHR) is of a diverse design to the other two trains (the SGs).

224 Westinghouse's design philosophy on AP1000 is to simplify the system design as much as possible. I agree with Westinghouse's concept of providing two safety systems which are functionally capable of performing the role and are qualified to the appropriate standard for safety systems so as to allow the level of redundancy in a the single safety system to be reduced. The claims on the two alternative sequences, bleed and feed and the start-up feedwater system, are discussed in the following paragraphs.

Sequence 1 – Claiming Bleed and Feed

225 In my GDA Step 3 report (Ref. 6), I noted that an important characteristic of the AP1000 design is that the ADS, in conjunction with the PXS, potentially provides an automated bleed and feed capability for loss of feed faults. On previous PWR designs, this function was performed manually and so it could not be claimed with the same reliability as is potentially possible for the AP1000. Such a feature would be a significant safety improvement on the previous generations of PWR designs, meeting, for example, the requirements of SAP ESS.8 by eliminating the need for operator action.

226 In its response to RO-AP1000-47 (Refs 29 and 66), Westinghouse has chosen to analyse a very conservative sequence in which, in addition to the failure of the PRHR, it has elected to considered the failure of the PMS. As was seen in the PMS failure sequence assessed in the previous section, the DAS can actuate the PRHR independently of PMS and so this is effectively assuming two common mode failures. Even assuming that a loss of normal feedwater occurs at a frequency of 0.1 per year (and ignoring the potential to claim the SFW system controlled by the PLS) this is clearly a very unlikely sequence given that the reliability of the PMS is 1×10^{-3} per demand and the failure of the PRHR is 2×10^{-4} per demand according to the PSA. Wishing to claim this sequence has caused Westinghouse to consider manual bleed and feed with limited time for operator action using the manual portion of the DAS system to open the ADS valves to promote depressurisation. Ideally, for design basis analysis demonstration I would wish to see significantly longer timescales available.

227 Westinghouse presents three transient analysis studies (Ref. 66) for this sequence. Following loss of both the MFW and SFW it also assumes the failure of the PRHR and the PMS, the base case assumes operator action to bleed and feed after 30 minutes. The second case assumes an additional common mode failure of the CMTs with operator action to bleed and feed after 30 minutes, while the third case presents a sensitivity study to the second case with the operator tripping after 40 minutes to explore cliff edge effects.

228 The calculations are performed with conservative design basis assumptions. An initial power level of 102% is assumed and conservative decay heat data at the 2-sigma level are assumed. Conservative initial pressures, temperatures and water volumes are assumed together with the thermal design flow. In practice, these assumptions will slightly shorten the time available for operator action but they will not significantly affect the outcome of the analysis in my judgement.

229 With the loss of all feedwater, all three cases initially start the same, with the DAS system tripping the turbine on low SG level at 62 seconds and the reactor at 67 seconds. The RCPs are tripped at 62 seconds and for the base case the CMTs are also actuated. The loss of feedwater and the turbine trip causes temperatures and pressures on both the primary and secondary sides to increase resulting in the PSVs and the SG MSSVs opening, thereby controlling the pressures at the set-points of the relief valves. Since the base case has the advantage of CMT recirculation during the initial phase of the transient, which mixes with and cools the coolant in primary circuit, the timescales for SG dry-out are delayed until about 1800 seconds. Indeed, for Case 1, the mass content of the primary circuit actually increases despite the PSVs being open. In contrast, Case 2 and Case 3 predict SG dry-out in about 800 seconds and the RCS quickly goes water solid causing the primary coolant mass to start to fall rapidly as coolant discharges through the PSVs. At the point when the operator actuates the ADS after 30 minutes, the primary coolant mass in the base case has increased from about 195 te to about 215 te. In Case 2, the primary coolant mass has decreased from about 195 te to about 80 te. In Case 3, after 40 minutes the primary coolant mass has decreased to about 58 te.

230 When the bleed and feed commences in Case 1, the fuel remains covered with water and does not heat up. In Case 2, with operator action at 30 minutes, the fuel is uncovered briefly such that the peak clad temperature reaches 403°C. In Case 3, with operator action 10 minutes later, the fuel is uncovered for longer such that the peak clad temperature reaches 847°C. This is still below the clad melt safety limit of 1204°C but is reaching the point where clad ballooning starts to become an issue, demonstrating that the operator could not delay his response much beyond 40 minutes if fault escalation is to be avoided. The base case illustrates the advantage of the CMTs being available as a source of additional coolant water. In Case 1, the timescale for operator action could certainly have been extended further, since the RCS inventory is still above its initial value at the time of ADS actuation.

231 All these sequences rely on operator action to actuate bleed and feed over relatively short timescales. In my opinion, 30 to 40 minutes is not very long given the decision the operator is required to make. For design basis analysis, where the requirement is to robustly demonstrate with high confidence any operator action, I would normally expect to see a demonstration of considerably longer time frames or ideally an automatic protection system as required by SAP ESS.8. Given the context of the likely sequence frequencies, the analysis is reassuring from a PSA perspective, suggesting that there is extra margin available for operator recovery even for these highly unlikely sequences. However, from design basis perspective, I would much preferred Westinghouse to have studied the more likely sequence of a loss of feedwater fault (including failure of the start-up feedwater system) with common mode failure of the PRHR but with the PMS remaining available to

automatically actuate ADS on low CMT level. Given the analysis that has already been presented (particularly for Case 1), I do not consider that this is a GDA Issue, but I have raised Assessment Finding **AF-AP1000-FS-23**, requiring a future licensee to perform this analysis and to establish whether automatic bleed and feed is feasible and if not to establish the timescales available for operator action to initiated bleed and feed for these more realistic design basis fault sequences.

232 The analyses for the bleed and feed cases that are presented were performed using RELAP-5. While this is a very well established thermal hydraulics computer code, no validation evidence for its applicability to the AP1000 design has been presented to HSE-ND to meet the requirements of SAPs FA.17 and FA.18. Hence, for this reason, I have raised Assessment Finding **AF-AP1000-FS-24**, for a future licensee to provide the validation evidence to support the use of the RELAP-5 code for application to AP1000 analysis or to make use of codes validated for the AP1000.

Sequence 2 – Claiming SFW System

233 It is noted that the design flow from a single SFW pump to the two SGs is 118 m^3/hr (or about 33 kg/s). This is very similar to the minimum auxiliary feedwater flow per pump of 114 m^3/hr (delivering to two SGs), that is provided on Sizewell B. The thermal power of the two reactors is identical at 3400 MW so the sizing of the start-up feedwater system appears to be sensible. It is also informative to perform an additional hand calculation for the heat balance at one hour. At this time, the reactor decay heat is about 1.5% or 51 MW. The RCPs contribute another 18 MW. The SGs will be held at a nominal pressure of 80 bara by the SG PORVs. Assuming feed enters at a temperature of 50°C then the enthalpy rise to saturated steam is 2758 kJ/kg – 216 kJ/kg = 2542 kJ/kg. Therefore the heat removal capacity of the two SGs is 2542 kJ/kg x 33 kg/s = 83,886 kW = 84 MW. Hence, even with the RCPs operating, the heat input of 69 MW is matched in less than one hour by the heat removal capacity of one start-up feedwater pump.

234 The functional capability of the start-up feedwater system is illustrated in a loss of off-site power transient reported in a design transient calculation note (Ref. 67) in support of a structural integrity assessment. Loss of off-site power results in the loss of normal feedwater system. The calculation is informative because it performs three calculations of the same transient using the LOFTRAN code. The base case (Case 1) utilises all the standard conservatisms that Westinghouse would traditionally apply in its safety analysis apart from claiming the SFW system.

235 Following a loss of off-site power, the reactor is assumed to trip as do the RCPs and there is a loss of normal feedwater. Unlike the EDCD analysis (Ref. 16), which credits the passive safety systems, the standby diesels and start-up feedwater system are credited to operate successfully. The initial conditions are 102% power with the thermal design flow. The initial mass of water in the SGs is at the low level reactor trip set-point and conservative Beginning of Life (BOL) moderator temperature coefficients are assumed. No credit is taken for the reactor power control system, the steam dump control system or the pressuriser pressure and level control systems. A two second delay is assumed between turbine trip and reactor trip and the SG PORVs are not credited initially so steam relief is through the MSSVs. The SG heat transfer area is minimised and the start-up feedwater system is assumed to take 120 seconds to deliver water to the SGs. The set pressure of the PSVs is 172.4 bara. The calculation predicts that the PSVs will lift with a maximum pressure of 175.1 bara.

236 The two sensitivity studies that have been performed remove key pessimisms from the analysis with the aim of demonstrating that the PSVs will not lift in practice. In the first

sensitivity case (Case 2), a correction is made to the decay heat model (conservative data appropriate for safety analysis is still used), the SG PORVs are assumed to operate, a nominal SG water level is used, and a best estimate BOL moderator coefficient is assumed. The changes have little effect and the calculation still predicts that the PSVs will lift with a maximum pressure of 174.1 bara. In the second sensitivity case (Case 3), the only change (relative to Case 2) is that the delay between the turbine trip and the reactor trip is reduced from two seconds to one second. No technical justification is given for this change and I have no feel for whether 1 second is still conservative. The calculation predicts that the PSVs will not lift with a maximum pressure of 168.9 bara. This would appear to still leave a significant number of conservatisms remaining in the analysis.

237 From the above discussion, I conclude that the SFW is adequately sized to ensure adequate removal of heat from the core, and together with the either the SG PORVs or MSSVs, is functional capable of providing a diverse heat sink to the PCS. It is noted that the SFW system is a Class A2 safety system and is located outside the containment building in the 1st bay of the turbine building. Improved segregation from other systems located in the turbine building has been provided through design changes proactively identified by Westinghouse during GDA Steps 3 and 4. The system is controlled by the PLS and powered by the ac electrical system with back-up power in the event of a loss of off-site power provided by the standby diesel generators which are also located outside containment. These are all Class A2 system systems. It looks demonstrably diverse from the Class A1 systems apart from the fact that it can be isolated by the PMS.

238 In addition, since the flow is governed by the PLS control system to the nominal value of 118 m^3/hr assumed in the transient analysis irrespective of the whether one or two pumps are operating (Ref. 68), the start-up feedwater system appears to have sufficient capacity, even assuming the single failure of one pump, to prevent the lifting of the PSVs following loss of off-site power fault. According to the response to TQ-AP1000-287 (Ref. 9), analysis performed for the PSA suggests it has sufficient capacity for the other loss of normal feedwater faults as well although these transients have not been subject to any assessment by HSE-ND. While lifting of a PSV is not strictly a safety criterion, it clearly eliminates the possibility of a consequential LOCA due to a stuck open PSV if the initial opening can be prevented in the first place for frequent faults such as a loss of off-site power. Given that TQ-AP1000-289 (Ref. 9) estimates that the conditional probability of a stuck open PSV is 1 x 10^{-2} per demand, this is a highly desirable feature since a stuck open PSV must be assumed to result in the conditional failure of the PRHR system. For this reason, Assessment Finding **AF-AP1000-FS-25** has been raised for a future licensee to provide analysis to confirm that the start-up feedwater system is adequately sized to ensure that the PSVs will not lift following the loss of normal feedwater fault (without loss of off-site power) since in this fault there will be a delay in the time to reactor trip while the mass of water in the SG reduces to the low SG narrow range trip set-point.

Loss of Normal Feedwater with Failure of CMT

239 In terms of pressuriser overfill it may be possible to demonstrate that a diverse safety system is not required to replace the function of the CMTs following an intact circuit fault such as a loss of normal feedwater fault. The CMTs initially provide a source of cooler water to mix with the warmer water in the RCS but in the long term they could make the transient more onerous since they will slightly increase the reactor coolant inventory for the fault possibly reducing the margin to overfill the pressuriser.

240 However, it must be recognised that the CMTs also provide an additional boration function which helps with long term shutdown requirements and provides a diverse means of shutdown following an ATWT event. In its response to RO-AP1000-47 (Ref. 29), Westinghouse argues that manual bleed and feed using manual ADS and IRWST injection can provide a diverse means of boration for the long term safety function. The CVS also provides a diverse Class A2 "other" means of achieving this function. Given the long timescales (many hours), I accept these arguments.

Loss of Normal Feedwater with Failure of PCS

241 The need for diversity extends to support systems. For this frequent fault, Westinghouse claims that both the primary and the diverse means of ultimate heat sink functions are provided by the PCS. Although the ADS together with the PXS provide diversity to the PRHR for the decay heat removal safety function, they also rely upon the PCS for the ultimate heat sink system. In its response to RO-AP1000-47 (Ref. 29), Westinghouse argues that the design of the PCS is remarkably robust against common mode failure. It is designed to withstand very limiting hazards. The actuation valves are of a diverse design, with the air operated solenoid valves failing safe in the event of a loss of off-site power meeting the requirement of SAP EDR.1. Westinghouse notes that there is an extended time frame available for actuation of the PCS in the case of non-LOCA intact circuit faults with large margins available until the peak design pressure of the containment vessel is reached. Large redundant drain lines are provided to reduce the likelihood of blockage. In a separate calculation performed in response to TQ-AP1000-348 (Ref. 9) in support of the PSA, Westinghouse also notes that the PCS may provide long-term cooling for non-LOCA events relying entirely on air cooling. The calculation is performed on a best estimate basis using a simplistic computer code although the key argument is based on the empirically derived heat transfer coefficients and the situation is essentially a steady-state condition. The design basis pressure limit for the containment vessel is exceeded but there is still margin available to the ultimate failure limit.

242 Westinghouse notes that the design has been subject to extensive independent peer review, although the response to RO-AP1000-52 (Ref. 35) erroneously states that the PCS performance has been confirmed by independent analysis performed by HSE-ND. As a sampling organisation, HSE-ND is not in a position to technically confirm the performance of the PCS since the GRS modelling work to which this comment refers was performed to aid the judgement of HSE inspectors and uses a heat transfer model that is not yet fully validated. The reference to HSE-ND will need to be removed from the response to RO-AP1000-52 (Ref. 35). In the UK it is for the vendor and licensee to assure them selves of the performance of a safety system such as the PCS. For this reason, Assessment Finding **AF-AP1000-FS-26** has been raised for a future licensee to ensure that this incorrect statement is removed in a revised response to RO-AP1000-52.

243 It is noted that the PSA assumes a reliability of 1.9×10^{-6} per demand for the PCS. However, SAP EDR.3 cautions against accepting claims for common cause failure reliability greater than 1×10^{-5} per demand suggesting that such a claim cannot be supported by currently available data and methods of analysis. Given the potential uncertainty in this claimed reliability figure, I have followed the HSE precautionary principle and focused my assessment on the two "other" diverse means of achieving the safety function on the AP1000 identified by Westinghouse to meet the requirements of SAPs EDR.2 and EDR.3.

244 Westinghouse's first diverse "other" means of achieving the ultimate heat sink function is through providing feed to the SGs from the start-up feedwater system with steam relief via the MSSVs. As noted above, the SFW system can be powered by the Stand-by Diesel Generators (SDG) should a loss of grid event be the cause of the loss of the normal feedwater fault. Actuation of the SFW system and the SDGs is automatically performed by the PLS. In its response to RO-AP1000-47 (Ref. 29), Westinghouse states that all these active systems are qualified as Class A2 safety systems and so they can be legitimately claimed to provide a diverse means of cooling within the design basis assessment in accordance with SAPs ECS.1 and ECS.2.

245 The functional capability of the SFW to provide adequate cooling has already been discussed above when considering the common mode failure of the PRHR. However, it must be recognised that both the normal feedwater and the SFW systems can be spuriously isolated by signals from either the PLS or the PMS and so it is important to demonstrate that a second means exists for providing the diverse ultimate heat sink function.

246 Westinghouse's second means is the RNS, which can be used to remove heat from the IRWST. The RNS is itself cooled by the component cooling water system (CCS) with the service water system (SWS) providing the ultimate heat sink function. This cooling chain can be powered by the stand-by diesel generators should a loss of grid event be the cause of the loss of the normal feedwater fault. The cooling chain is aligned and actuated by the operator using the PLS. Given the large thermal capacity of the IRWST, the operator has roughly two hours before the IRWST starts to boil to achieve this action although it is recognised that this is not a cliff edge. Again, Westinghouse's response to RO-AP1000-47 (Ref. 29) states that all these active systems are qualified as Class A2 safety systems and so they can be legitimately claimed as providing a diverse means of cooling within the design basis assessment in accordance with SAPs ECS.1 and ECS.2.

247 Westinghouse has provided some calculation notes (Refs 69 and 70) in order to substantiate that the RNS / CCS / SWS cooling chain is adequately sized for this safety functional requirement. The main sizing calculation (Ref. 69) states that it applies to the AP1000 design for a non UK site while the other supporting reference (Ref. 70) contains a number of open items. The main sizing calculation (Ref. 69) states that the calculations are not to support safety analysis and so no train failures are assumed. However, given that its role is to provide a diverse means of protection and the single failure criterion only applies at the functional rather than the system level this is not necessarily an issue although this might have implications with regard to preventative maintenance activities due to plant availability requirements within the Technical Specifications.

248 The calculation appears to be performed on a very conservative basis with no credit taken for any heat removed by the SGs as they dryout (my judgement is that they would be capable of removing the majority of the decay heat for at least the first 30 minutes following reactor trip). The calculation assumes that the RNS commences cooling of the IRWST after two hours. The aim of the calculations is to size the heat exchangers on the CCS and SWS and the cooling tower such as to be sufficient to prevent the IRWST from boiling. The calculation concludes that for the design parameters selected, the RNS is capable of preventing boiling in the IRWST, with the temperature peaking at 94°C after one hour (i.e. 3 hours after reactor trip). The calculation sizes the proposed RNS heat exchanger design to have a heat removal capacity of about 36 MW. Since I estimate that the decay heat will be about 51 MW one hour after the reactor has tripped, this requirement appears reasonable.

249 Recognising the preliminary nature of these calculation notes (Refs 69 and 70) and that the detailed design of these systems is still to be performed for the UK design, I have

raised Assessment Finding **AF-AP1000-FS-27**, for the future licensee to ensure that the final design of the RNS, CCS and SWS systems is sized sufficiently to ensure they are capable achieving this diverse safety function identified for them in response RO-AP1000-47 (Ref. 29). As part of the assessment finding, the licensee shall consider whether it is ALARP to increase the sizing to provide extra capacity to allow for plant maintenance activities on a single train. It is also noted that the calculation discussed above was only performed for intact circuit faults. Given that the sizing of these systems can potentially affect plant layout, this assessment finding will need to be completed before the pouring of the first nuclear island safety related concrete.

250 The response to RO-AP1000-47 (Ref. 29) also identifies that these systems can perform this role for SBLOCA faults discussed in Section 4.2.8 below. As SBLOCA faults will release additional stored energy to the IRWST (in the form of sensible heat contained in the RCS) when the ADS Stages 1 to 3 are discharged, the sizing requirements for the cooling chain are likely to be slightly more demanding and yet no supporting calculations have been provided to support the claim for this function. The scope of Assessment Finding **AF-AP1000-FS-27** is therefore extended such that the future licensee will need to demonstrate that the RNS, CCS and SWS systems are adequately sized for SBLOCA faults as well.

Loss of Normal Feedwater with Failure of PSVs

251 A significant feature of the loss of normal feedwater transient is that pressuriser safety relief valves lift twice during the transient (once during the pre-trip transient until terminated by reactor trip and once during the post-trip transient due to SG dry-out) as illustrated in Fig 15.2.7-5 of the EDCD (Ref. 16). This has two potential consequences that need to be considered within the design basis. The first is that the PSVs could fail to open due to a common mode failure. The second is that a consequential LOCA could occur should one of the safety relief valves fail to close on demand. As I noted in the discussion of the inadvertent closure of all MSIVs fault in the previous section, this contrasts with the situation at Sizewell B which is provided with three Pilot Operated Safety Relief Valves (POSRV) and a diverse set of two spring loaded Pressuriser Safety Relief Valves (PSRV) to provide some additional protection against both these possibilities. Westinghouse argues the possibility of consequential LOCA is acceptable and bounded by the transient for the inadvertent opening of the PSV design basis fault already presented in the EDCD. This argument is discussed further in the next sub-section on consequential failures.

252 Failure of the PSVs to lift during the pre-trip transient for the loss of normal feedwater fault is bounded by the inadvertent closure of both MSIVs fault as discussed in Section 4.2.3.2 above: the latter is a much more onerous transient since the reactor heats up significantly more before the reactor trip signal is generated. However, in the case of the AP1000, the primary means of decay heat removal following loss of normal feedwater is through natural circulation cooling using the PRHR. The sizing of the PRHR is such that its heat removal capacity is insufficient to avoid an initial heat-up of the primary circuit following reactor trip as the SGs dry out due to the assumed initiating event. The heat-up continues until the decay heat has fallen to a level matching the heat removal capabilities of the PRHR. This post-trip heat-up transient causes the PSVs to lift for a second time.

253 In my judgement, given that the loss of normal feedwater and start-up feedwater systems can occur as a result of the same initiating event due to failures in either the PLS or the PMS, this transient must be regarded as a frequent event for which common mode failure

of the PSVs needs to be considered. Although Westinghouse has considered common mode failure of the PSVs following the inadvertent closure of both MSIVs fault, there is no discussion of the potential for common mode failure of the PSVs to open following the loss of normal feedwater fault during the post-trip transient.

254 The pressuriser water volume transient for loss of normal feedwater is presented in Fig 15.2.7-6 of the EDCD (Ref. 16). Although Westinghouse accepts that this is a much higher frequency event than the feedline break discussed in Section 4.2.3.1 above, the transient is remarkably similar to the equivalent plot in Fig 15.2.8-6 for the feedline break. The only significant difference is that both SGs are intact and so they both contain water during the early stages of the transient. This tends to delay the transient slightly rather than significantly altering the margin to fill on pressuriser water level. The concern is that should the PSVs fail to lift, the steam space in the pressuriser will be compressed and could challenge the structural integrity limit of 221 bara. Operator action to actuate ADS or open the head vent valves potentially provides a diverse means of pressure control although it is not clear that the 30 minute rule for operator actions set out in SAP ESS.9 will be met. For this reason, Assessment Finding **AF-AP1000-FS-28** has been raised requiring a future licensee to confirm the adequacy of the diverse protection for this fault.

4.2.3.6 Consequential Failures

255 No discussion is presented within the analyses about the possibility of consequential failures such as a stuck open pressuriser safety relief valve resulting in a consequential LOCA or SGTR failures following a feed line break. This is perhaps unsurprising given that this design transient section is attempting to demonstrate that the sizing of the PRHR is adequate. Nevertheless, given that the conditional failure probability for a safety relief valve to close is typically 1×10^{-2} per demand, there is a case for considering such sequences to be within the design basis (in accordance with SAP FA.5) depending upon the frequency of the initiating event. For this reason, TQ-AP1000-837 was raised requesting Westinghouse to provide additional arguments or analysis to justify its position.

256 In its response to TQ-AP1000-837 (Ref. 9), Westinghouse has reviewed all the design basis faults that are associated with intact circuits and which could result in the lifting of the PSVs. The events considered are:

- all of the decrease in heat removal faults;
- the uncontrolled RCCA bank withdrawal fault;
- the RCCA ejection accident;
- the RCP seizure and shaft break faults, and;
- the increase in reactor coolant inventory faults.

Westinghouse argues that of these faults, the most limiting are the feedline break fault and loss of AC power fault, and that these events are themselves bounded by either the spurious opening of the pressuriser safety valve design basis fault in the short-term or the inadvertent operation of the ADS design basis fault in the long-term. In the case of the short term transient, this is because the reactor is tripped in response to the initiating event before the valve has chance to fail in the open position. Essentially, all the plant parameters are unchanged from the nominal conditions apart from the power level, since the reactor is already tripped, and the pressure which is slightly higher. The latter two effects are beneficial in terms of DNB. In the case of the long-term transient, not only has

the reactor been tripped by the initiating event but the CMTs have also been activated prior to the break occurring when compared with the spurious ADS event.

257 I accept these arguments provided that the cause of the initiating event is not a spurious C&I signal from the PMS (e.g. normal feedwater isolation), since in such circumstances the PMS should not be assumed to be available to protect against the consequential LOCA event it has caused. Westinghouse is making the implicit assumption that the PMS is available in this response. The issue of spurious PMS initiation is discussed further in Section 4.2.10.4 below where Assessment Finding **AF-AP1000-FS-51** is raised for a future licensee to provide a safety case for such events.

4.2.3.7 Controlled State to Safe Shutdown State

258 In its response to RO-AP1000-52 (Ref. 35), Westinghouse's treatment of decrease in heat removal faults is identical to that for the increase in heat removal faults discussed in the previous section. Essentially, Westinghouse argues that decrease in heat removal faults fall into the intact circuit fault group.

259 As with the case of increase of heat removal faults, the Westinghouse response is not sufficiently detailed to provide an adequate final safety case with regard to each specific fault within the decrease in heat removal fault class. In particular, no attempt is made to identify specific operator actions required for individual faults. For example, with the feedline break fault, there may be a need, as with the steamline break faults, for the operator to ensure the isolation of the affected SG and to conserve feed stocks. Hence, Assessment Finding **AF-AP1000-FS-16** is seen to also be applicable to these faults. In addition, it must be recognised that decrease in heat removal faults are the limiting fault class in terms of decay heat removal function for intact circuit faults. It is therefore important that the issue of the definition of safe shutdown state raised under Assessment Finding **AF-AP1000-FS-04** above is closed out to confirm the adequacy of the passive cooling systems to reach the safe shutdown state.

4.2.3.8 Radiological Consequence Assessment

260 SAPs FA.3 and FA.7 require that a radiological consequence analysis, on a conservative basis, should be performed for each design basis fault sequence that can lead to the release of radioactive material. As discussed in the Section 4.2.2.8 above, Westinghouse has had to revise its radiological consequence assessment in response to RO-AP1000-48 which requested an assessment of the radiological consequences of design basis faults against the UK requirements given in SAPs FA.3, FA.7 and Target 4.

261 A detailed review of the radiological consequence analysis methodology applied by Westinghouse in its response to RO-AP1000-48 is presented in Section 4.6 below. The conclusion of this review is that in general the radiological consequences methodology appears sensible and conservative but that in some areas further justification will be required as part of site licensing process. On this basis, it is my judgement that the methodology presented in the RO-AP1000-48 response (Ref. 50) is broadly appropriate for this preliminary Step 4 GDA assessment of individual faults against Target 4 in the HSE SAPs given that Action 2 of GDA issue **GI-AP1000-FS-02** requires Westinghouse to demonstrate that the radiological consequence analysis is appropriate for the UK design reference point (see Section 4.6 below).

262 The response to RO-AP1000-48 (Ref. 50) argues that the consequences of a loss of normal feedwater flow fault and the inadvertent closure of the main steam isolation valve fault can be bounded by the release from the loss of off-site power fault. This is also a

Condition II event. Westinghouse argues that this sequence is bounding even though the relief valves are assumed to operate normally because a stuck open relief valve on the AP1000 plant results in the affected SG being isolated. In contrast, if the safety relief valves operate normally, they continue to open and close for an extended period. This claim has not been assessed during Step 4 but can be reviewed as part of the closure of Action 1 of GDA Issue **GI-AP1000-FS-02**. The predicted radiological release from the loss of off-site power fault is 0.05 mSv which comfortably meets the BSL limit of Target 4.

263 Westinghouse has decided to bound the radiological assessment for the main feedline break fault by the radiological release determined for the main steamline break fault discussed in Section 4.2.2.8 above (Ref. 119) of 5.6 mSv. Although this represents a conservative assumption it must be recognised that the assumed frequency for a feedline break at 4×10^{-4} per year is higher than that for the steamline break and so corresponds to a Target 4 BSL limit of 10 mSv. This leaves a relatively small margin to the BSL limit. However, the radiological assessment report (Ref. 119) notes that the initiating frequency for a feedline break fault is an open item that is being reviewed. This issue will therefore also need to be revisited as part of Action 2 of GDA Issue **GI-AP1000-FS-02** when Westinghouse will be required to confirm the adequacy of the radiological assessments as discussed in Section 4.6 below.

4.2.3.9 Findings

264 Following my assessment of the decrease in heat removal faults, I am broadly content with the fundamental design of the AP1000 to protect against this class of fault. It is judged that the sizing of the SGs, PRHR, CMTs, PSVs, PCS and the MSSVs on the AP1000 are sufficient to provide adequate protection against this class of faults. I am particularly impressed with the validation test work performed to justify the functional performance of the passive systems, which in my view is world class. It must be recognised that while the sizing of the PRHR is sufficient to perform its role of decay heat removal, it is not functionally capable of preventing the PSVs from lifting. For faults resulting in overpressure transients such as loss of normal feedwater faults, the failure probability of the system will be limited by the conditional probability of the PSVs to reseat and will therefore be relatively modest by Class A1 safety system standards. This emphasises the importance of the Class A2 SFW system and its support systems, such as the standby diesel generators, as a risk reduction measure.

265 My one remaining concern with the passive systems is the functional capability of the condensate return gutter to maintain sufficient water inventory within the IRWST for the period of 72 hours claimed within the safety case. For this reason, GDA Issue **GI-AP1000-FS-06** has been raised for Westinghouse to demonstrate the functional capability of the IRWST to adequately cool the PRHR following actuation.

266 Further reassurance is required on the sizing of the SG PORVs in their role in providing the diverse means of preventing SG over-pressurisation following the spurious MSIV closure fault with common mode failure of the MSSVs. This has been raised under Assessment Finding **AF-AP1000-FS-21**.

267 I am satisfied that the sizing of the SFW system is sufficient to ensure it can perform its role as a diverse means of decay heat removal and a diverse means of ultimate heat sink. Nevertheless, from an ALARP perspective in terms of reducing risk, there are considerable advantages in ensuring that it is sufficiently sized to avoid the PSVs lifting during a loss of feedwater or a loss of off-site power fault. Westinghouse claim this has been done but the analysis has not been provided to HSE-ND. For this reason,

Assessment Finding **AF-AP1000-FS-25** has been raised for a future licensee to provide this information.

268 Further reassurance is required on the sizing of the RNS, CCS and SWS in their role as a diverse "other" means of providing an ultimate heat sink under Assessment Finding **AF-AP1000-FS-27** although I accept that the design intent as demonstrated by the RNS sizing calculations is for this to be case for intact circuit faults. Given that this assessment finding could potentially affect plant layout, I have asked that it be closed out prior to the pouring of nuclear island safety related concrete.

269 Further reassurance is also required on the sizing of the pressuriser following the loss of normal feedwater fault with common mode failure of the PSVs under Assessment Finding **AF-AP1000-FS-28**. Although this is less likely to affect plant layout, it is significant and so I have asked for this finding to also be closed out prior to the pouring of nuclear island safety related concrete.

270 The remaining assessment findings are items requiring further confirmatory analysis or support from commissioning tests rather than a fundamental issue with the design and in my judgement they can be closed out as part of the site licensing process.

4.2.4 Electrical Supply Faults

4.2.4.1 Summary of Westinghouse's Safety Case

271 Faults in this category result in the total or partial loss of normal on-site electrical ac supplies. Such faults include the loss of off-site power, the total or partial loss of on-site supplies, the loss of main generator synchronism, and a reduction in grid frequency.

272 Westinghouse has already explicitly considered many of these faults within other fault categories. For example, the long term decay heat removal aspects of the loss of external electrical load fault and the loss of ac power to station auxiliaries fault are considered in the decrease in heat removal faults discussed in Section 4.2.3 above, while the short-term fuel cooling aspects associated with the complete loss of reactor coolant flow fault caused by the loss of off-site power are considered in the decrease of reactor coolant system flow rate faults discussed in Section 4.2.5 below.

273 The basis of the Westinghouse safety case is that following loss of off-site power with turbine generator trip, the on-site standby ac power system supplied by the Class A2 diesel generators remains available to power the active Class A2 safety systems such as the CVS, SFW, RNS, CCS and SWS. Should a common mode failure of the on-site standby ac power system occur for whatever reason, the passive Class A1 safety systems are the primary means of bringing the plant to safe shutdown conditions. Importantly, although the Class A1 dc batteries automatically supply power to the Class A1 dc power distribution network, for intact circuit faults these batteries are not required: the reactor trip and actuation of the PRHR, CMTs and PCS will automatically occur on loss of dc power as this is their fail-safe mode. These systems are able to provide the decay heat removal, the long-term reactivity control and the ultimate heat sink functions. If the Class A1 dc power is not lost then the Class A1 PMS remains available to automatically trip the reactor and actuate the these passive systems on low SG level.

4.2.4.2 Assessment

274 The at-power reactor safety case following loss of electrical system faults is a particularly strong aspect of the overall AP1000 design. For a reactor at power, the primary means of achieving the main safety functions following loss of off-site power are provided by class

A1 passive safety systems that can automatically perform their intended safety function without the need for any electrical power (ac or dc) in a fail-safe mode for up to 72 hours. This is judged to meet the requirements of SAPs ESS.8, EDR.1 and EKP.2. In addition, following loss of off-site power, a diverse means is provided for each of the main safety functions, either by a diverse Class A1 passive safety system or by "other" diverse active Class A2 safety systems. This is judged to meet the requirements of SAPs EDR.2, EDR.3 and EDR.4.

275 As noted in Section 4.1.7 above, the PSA assessment of AP1000 (Ref. 19) has identified the need under Assessment Finding **AF-AP1000-PSA-13** for a review of the PSA to see if any additional electrical system faults need to be included in the list of initiating events. For this reason, Assessment Finding **AF-AP1000-FS-06** has been raised for a future operator to consider the findings of this review, and to see if any additional initiating events need to be included within the list of design basis events to meet the requirements of SAPs FA.4 and FA.5. However, in my judgement this is unlikely to be the case.

4.2.4.3 Findings

276 As noted in Section 4.1.7, Assessment Finding **AF-AP1000-FS-06** requires a future licensee to review any electrical system faults identified from the PSA review performed under Assessment Finding **AF-AP1000-PSA-13** as potential candidates for treatment as design basis faults.

4.2.5 Decrease in Reactor Coolant System Flow Rate Faults

4.2.5.1 Summary of Westinghouse's Safety Case

277 Faults in this category result in a reduction of flow in the primary circuit potentially resulting in a reduction of cooling to the fuel such that it undergoes DNB. The challenge is to trip the reactor before significant fuel damage can occur.

278 The basis of Westinghouse's safety case is that it has reviewed a number of postulated events that it considers to be within the design basis of the plant and that could result in a decrease in the RCS flow rate. For those cases which it considers to be limiting, it has performed detailed analyses and claims to have demonstrated that even for the most bounding faults the PMS is able to trip the reactor sufficiently quickly to avoid significant fuel damage. In particular, Westinghouse claims that each RCP includes sufficient internal rotating inertia to provide a flow coast down that avoids DNB following a loss of reactor coolant flow accident.

4.2.5.2 Assessment Overview

279 Westinghouse has considered the following faults within this category that it considers to be limiting and which are presented within the EDCD:

- partial loss of forced reactor coolant flow;
- complete loss of forced reactor coolant flow;
- reactor coolant pump shaft seizure (locked rotor), and;
- reactor coolant pump shaft break.

280 The first event is a Condition II event, the second a Condition III event, and the last two events are Condition IV events according to Westinghouse's classification scheme. I have chosen to sample the second fault listed above because the design of the RCPs is

different on AP1000 compared with conventional PWR plant and so the fault is potentially more onerous. In addition, although it is a Condition III event, loss of electrical supplies to the pumps could be a possible cause of the fault and so I judge that the initiating frequency will be close to a Condition II event.

4.2.5.3 Assessment of Complete Loss of Forced Reactor Coolant Flow (Limiting Frequent Fault)

Fault Sequence Analysis

281 This fault considers the loss of reactor coolant flow as a result of the simultaneous coasting down of all four RCPs. The fault is treated as a design basis transient and so meets the requirement of SAP FA.5. There are multiple redundancies provided within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met.

Methods and Assumptions

282 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling the complete loss of forced reactor coolant flow fault, Westinghouse has made the following assumptions to ensure a robust and conservative assessment.

- Nominal initial conditions are assumed in accordance with the revised thermal design procedure. Uncertainties in the initial conditions are instead included in the DNBR limit.
- The minimum moderator density coefficient is assumed.
- The maximum Doppler coefficient is assumed.
- The axial power shape assumed in the analysis for the DNB calculation performed by VIPRE-01 is a chopped cosine with an appropriately conservative peak to average value. The full power radial peaking factor, $F_{\Delta H}$, assumed is 1.59.
- The curve of trip reactivity insertion versus time is based on a 2.09 second RCCA insertion time to the dashpot appropriate for all coolant pumps coasting down. Drop time testing requirements will be specified in the Technical Specifications.
- The fraction of total negative reactivity insertion versus normalised RCCA position assumed is based upon a core where the axial distribution is skewed to the lower region of the core. An axial distribution skewed to the lower region of the core can arise from an unbalanced xenon distribution. This curve is used to compute the negative reactivity insertion versus time following a reactor trip, which is input to the point kinetics core models used in the transient analyses. The bottom skewed power distribution itself is not an input into the point kinetics core model. This is an inherent conservatism since for cases other than those associated with unbalanced xenon distributions, significantly more negative reactivity is inserted than that assumed in the curve due to the more favourable axial distribution existing prior to trip.
- The set-point values include instrumentation and set-point uncertainties and the maximum time delays are assumed within the analysis.
- A conservative flow coast-down transient is used.

283 The Westinghouse analysis uses the LOFTRAN, FACTRAN and VIPRE-01 computer codes to model these decrease in flow rate faults. The assessment of VIPRE-01 code against the validity of assurance SAPs FA.18 to FA.22 is reported in the fuel and core assessment (Ref. 17). The general assessment of the LOFTRAN code is reported in Section 4.3.4. The LOFTRAN code uses a point kinetics model for the analysis of these faults. The critical heat flux correlations used by the VIPRE-01 code to determine whether the fuel enters DNB during the transient are based upon the AP600 low-flow CHF test data analysis report (Ref. 71). The CHF correlation and the associated uncertainties required by the revised thermal design procedure (Ref. 72) ensure there is at least a 95% probability at the 95% confidence level that DNB will not occur on the most limiting fuel rod during normal operation and fault conditions. This has also been reported in the fuel and core assessment (Ref. 17), which concludes that the methods used for the prediction of CHF are satisfactory.

284 These methods and assumptions are generally consistent with standard design basis approaches to such faults and are comparable to those applied in the Sizewell B analysis. They are judged to result in a bounding assessment meeting the requirements of SAP FA.7.

Transient Analysis

285 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. In practice, for the faults considered in this section, the aim of Westinghouse is to demonstrate that this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB. To confirm that these objectives have been achieved, the results of design basis analysis of Westinghouse for these faults are reviewed.

286 The transient analysis focuses on demonstrating that the protection system can trip the reactor quickly enough to avoid the fuel going into DNB. The fault is a race between the speed of the RCPs coasting down and the speed of the protection system and the RCCAs to insert. Although the transient analysis is important, many of these parameters can be confirmed during commissioning tests that are proposed for each reactor prior to operation.

287 The analysis results are presented Fig 15.3.2-6 of the EDCD (Ref. 16). The minimum DNBR shown suggests that there is adequate margin to DNB. However, these transients are very sensitive to the initial starting conditions of the fault. Perturbations in the grid frequency (which could potentially be linked with the initiating event) may also result in the RCPs operating at a reduced initial speed. In addition, the reactor power level and the axial and radial power distribution may become distorted as the control system responds to the grid frequency variations. Westinghouse argues that the frequency inverter required on the UK design will limit the variation in RCP speed during grid perturbations although no evidence has been provided to quantify this effect. There is a need to perform some transient analysis to study these effects. For this reason, the resolution plan for Action 5 of GDA Issue **GI-AP1000-FS-03** requires Westinghouse to identify the limits and conditions of operation for this fault to ensure that the fuel does not enter DNB. As part of this action, Westinghouse will need to consider the effects of the turbine governor valve increasing the initial reactor power in response to a perturbation on the grid frequency.

288 A related matter is that as part of the initial test programme described in Chapter 14 of the EDCD (Ref. 16), Westinghouse is proposing a load-follow demonstration only on the first AP1000 plant to be commissioned. This proposal is not considered to be adequate recognising that the turbine control systems for any UK plant are likely to be UK specific. For this reason, Assessment Finding **AF-AP1000-FS-29** has been raised requiring a future licensee to perform such a demonstration for the first of a kind UK design.

289 While Westinghouse has categorised the complete loss of forced reactor coolant flow as a Condition III event, the initiating frequency is high enough for it to be considered frequent within the traditional UK approach to design basis analysis, with the requirement for two diverse safety systems to be provided for each safety function. In its response to RO-AP1000-47 (Ref. 29), Westinghouse has identified the following limiting fault sequences that need to be assessed to demonstrate that the AP1000 has diverse means of achieving each safety function:

- Loss of forced reactor coolant flow with failure of RCCAs to insert, and;
- Loss of forced reactor coolant flow with failure of PMS to trip the reactor.

290 In practice, Westinghouse has chosen to perform a combined analysis of these sequences in which the RCCAs are assumed to fail to insert and PMS fails such that reactor trip (which fails) and turbine trip are actuated by the DAS using the high hot leg temperature trip signal. Westinghouse argues that the other potential fault sequences associated with this fault are bounded by the loss of normal feedwater fault discussed in Section 4.2.3 above. I accept this argument because tripping the RCPs reduces the heat removal requirements of the post-trip cooling systems. The transient analysis performed in support of the combined fault sequence is discussed below.

Loss of Forced Reactor Coolant Flow with Failure of PMS and RCCAs to Insert

291 As with the loss of feedwater ATWT case with failure of the RCCAs to insert considered in Section 4.2.3.5 above, Westinghouse has performed a largely best-estimate analysis for the loss of forced reactor coolant flow fault with a failure of the reactor to shutdown. The plant initial conditions reflect nominal full power values and no measurement or instrumentation errors are assumed. BOC reactivity coefficients are assumed since this is known to be the most onerous point of the fuel cycle for ATWT analysis. The comments in Section 4.2.3.5 about the different moderator feedback assumptions made in the loss of feedwater ATWT case between the EDCD (Ref. 16) and those assumed in current analysis (Ref. 47) that resulted in Action 2 of GDA Issue **GI-AP1000-FS-02** and Action 1 of GDA Issue **GI-AP1000-FS-03** are equally applicable here. The analysis is performed with the LOFTRAN computer code using its point kinetics model and the identified design limit is to prevent the fuel from entering DNB.

292 The results presented for the fault (Figures 7.3-8a to 7.3-12, Ref. 47) show that the reduction in flow causes a rapid reduction in core power as the moderator density reduces and the RCS pressures and the temperatures increase. As noted above, the low RCP under-speed reactor trip signal on PMS is not modelled. Indeed the high hot leg temperature trip on DAS is not modelled either, because by the time that trip parameter is reached the minimum DNB value is already predicted to have occurred (at about 5 seconds) based on the WRB-2M CHF correlation.

293 The minimum DNBR transient is plotted in Fig 7.3-11 of the report. Two correlations are plotted because of concerns about the validity of the correlations for the given fault conditions, although Westinghouse claims the WRB-2M CHF correlation remains within its validation range over the period of interest where the minimum occurs. The variation in

DNBR from its initial value is very similar to the transient for the reactor trip case reported in Figure 15.3.2-6 of the EDCD (Ref. 16). The DNB transient in the reactor trip case varies from roughly 2.6 to 1.4 over a period of about 3 seconds when the RCCAs insert in response to the RCP under-speed trip on PMS. The DNB transient in the ATWT case varies from roughly 2.6 to 1.6 but over a period of about 6 seconds. Insufficient information is provided to make an informed independent judgement as to why this should be the case.

294 As noted above, the calculation is started from nominal reactor conditions. No consideration is given to the effects of grid frequency perturbations on reactor power, axial off-set or radial peaking factor. Insufficient information is given to understand the differences in the calculations performed for the EDCD (Ref. 16) and those within the RO-AP1000-51 (Ref. 47) response. Sizewell B is provided with a RCP underspeed trip on both its primary protection system and its diverse secondary protection system. AP1000 is provided with an RCP underspeed trip on the PMS only. Sizewell B has a lower peak linear rating than AP1000 and the RCP coastdown is slower. I am therefore still to be convinced that the AP1000 does not need such a trip parameter on the DAS. For this reason, I require Westinghouse to better explain its safety case in this area through the response to Action 5 of GDA Issue **GI-AP1000-FS-03** on functional diversity. This requires Westinghouse to demonstrate that there are adequate trip parameters on the DAS to protect against a complete loss of forced flow fault.

4.2.5.4 Controlled State to Safe Shutdown State

295 As noted above, the long term aspects of this fault class are covered by the loss of external electrical load fault and the loss of ac power to the station auxiliaries fault which are part of the decrease in heat removal faults discussed in Section 4.2.3 above.

4.2.5.5 Radiological Consequence Assessment

296 SAPs FA.3 and FA.7 require that a radiological consequence assessment, on a conservative basis, should be performed for each design basis fault sequence that can lead to the release of radioactive material. As discussed in the previously in Sections 4.2.2.8 and 4.2.3.8 above, Westinghouse has had to revise its radiological consequence assessment in response to RO-AP1000-48. A detailed review of the radiological consequence assessment methodology applied by Westinghouse in its response to RO-AP1000-48 is presented in Section 4.6 below. The conclusion of the review is that in general, the radiological assessment appears sensible and conservative but that in some areas further justification will be required as part of site licensing process. On this basis, it is my judgement that the methodology presented in the RO-AP1000-48 response (Ref. 50) is broadly appropriate for this preliminary Step 4 GDA assessment of individual faults against Target 4 in the HSE SAPs.

297 The response to RO-AP1000-48 (Ref. 50) provides an explicit assessment of the radiological release from the loss of off-site power fault. The predicted release for the loss of off-site power fault is 0.05 mSv which comfortably meets the BSL limit of Target 4 for a Condition II event (which is clearly more restrictive than a Condition III event).

4.2.5.6 Findings

298 I have raised Action 5 of GDA Issue **GI-AP1000-FS-03** on functional diversity for Westinghouse to demonstrate adequate diverse protection for the complete loss of forced reactor coolant flow fault. The one Assessment Finding, **AF-AP1000-FS-29,** is with

regard to a functional test of the load following capability of the AP1000 and can be closed out during site licensing as part of the commissioning programme for the AP1000.

4.2.6 Reactivity and Power Distribution Anomalies

4.2.6.1 Summary of Westinghouse's Safety Case

299 Faults in this category cause the fuel to generate power in excess of the cooling provisions. Such faults can be brought about by, for example, a single RCCA withdrawal, withdrawal of banks of RCCAs, or reduction in the degree of boration in the primary circuit.

300 The basis of Westinghouse's safety case is that it has reviewed a number of postulated events that it considers to be within the design basis of the plant and that could result in reactivity and power distribution anomalies. For those cases which it considers to be limiting it has performed detailed analyses and demonstrated that even for the most bounding faults the PMS is able to detect the fault and trip the reactor sufficiently quickly to either prevent DNB or avoid significant fuel damage.

301 In performing the transient analysis, Westinghouse has, where relevant, performed sensitivity studies on the size of the moderator reactivity feedback coefficient, the initial power level, and the effects of the availability of offsite power following reactor trip, which potentially results in the tripping of the RCPs. On the basis of the analysis presented, Westinghouse has concluded that adequate protection is provided for all the range of faults considered.

4.2.6.2 Assessment Overview

302 Westinghouse has considered the following faults within this category that it considers to be limiting and which are presented within the EDCD:

- uncontrolled RCCA bank withdrawal from a subcritical or low-power start-up condition;
- uncontrolled RCCA bank withdrawal at power;
- RCCA misalignment;
- start-up of an inactive reactor coolant pump at an incorrect temperature;
- CVS malfunction that results in a decrease in the boron concentration in the reactor coolant;
- inadvertent loading and operation of a fuel assembly in an improper position, and;
- spectrum of RCCA ejection faults.

303 Most of the faults listed above are Condition II events. Inadvertent misloading is a Condition III event while RCCA ejection faults are a Condition IV event. RCCA misalignment includes both Condition II and Condition III events. Having reviewed all the faults, five have been chosen for a sample assessment.

- The first is the uncontrolled RCCA bank withdrawal at power fault since it is a frequent fault which challenges the coverage of the protection system over a wide range of initial powers and reactivity insertion rates, as well as the integrity of the fuel due to PCI failures.

- The second fault is the RCCA misalignment fault on the grounds that it is a difficult fault for the automatic protection to detect. The overtemperature ΔT trip appears to provide the only means of automatic protection.
- The third is CVS malfunction resulting in a decrease in the boron concentration in the reactor coolant since this can be difficult to protect against in shutdown conditions without adequate flux protection.
- The fourth is the inadvertent misloading faults since the protection for such faults is largely reliant upon administrative control.
- The final fault is the RCCA ejection fault which Westinghouse judges to be the most bounding case in terms of fuel damage.

4.2.6.3 Assessment of Uncontrolled RCCA Bank Withdrawal at Power

304 Westinghouse has treated uncontrolled withdrawal of an RCCA bank at power as a design basis transient. The requirements of SAPs FA.4 and FA.5 are met. Westinghouse claims that there are multiple redundancies within the PMS for these faults and that the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 have also been met. The transient analysis focuses on demonstrating that the protection system can trip the reactor quickly enough to avoid the fuel going into DNB. The fault is a race between the rate of increase of the core power and temperature as the RCCA bank is withdrawn and the speed of the protection system to trip the reactor and cause the RCCAs to insert. As this is a frequent fault, I have examined the provision of diversity to protect against this fault.

305 Westinghouse claims that the following protection systems are available to protect against this fault:

- reactor trip on high-power range neutron flux (ex-core detectors);
- reactor trip on high-power range positive neutron flux rate (ex-core detectors);
- reactor trip on overtemperature ΔT (DNB protection);
- reactor trip on overpower ΔT (linear rating protection);
- reactor trip on high pressuriser pressure;
- reactor trip on high pressuriser level.

306 The overtemperature ΔT and overpower ΔT protection systems are both derived from measurements of the pressuriser pressure and the coolant temperature in the hot and cold legs and the axial offset determined using the ex-core detectors.

307 In my GDA Step 3 report (Ref. 6), I noted that Sizewell B has both a primary protection system (PPS) and secondary protection system (SPS) through which the following trip parameters are claimed: high cold leg temperature, high positive flux rate (PPS), high positive flux rate (SPS), high flux (PPS) and high N-16 (PPS). I also noted that Sizewell B is provided with diverse flux protection signals on both the PPS and SPS. The DNBR core limit trip, which is a roughly equivalent to the overtemperature ΔT trip on AP1000 (although the Sizewell B trip signal is based upon N-16 detectors rather than the ex-core detectors for the AP1000), is not claimed. The N-16 system is provided for over-power trip protection against cool-down faults due to concerns about the calibration of the ex-core detectors in such faults as discussed above. However, this system also provides diverse over power protection to the high-flux ex-core detection system. The AP1000 does not possess such a system. However, it does possess in-core detectors although

these are not connected to the protection system and so cannot trip the reactor automatically. Hence, there appears to be no diversity for high-flux reactor trip protection on the AP1000, so that the requirements of SAP ESS.7 are not met. During GDA Step 4, in its responses to RO-AP1000-47 (Ref. 29) and RO-AP1000-51 (Ref. 47), Westinghouse has proactively identified the need for a design change to provide diverse protection against this fault using a new high hot leg temperature reactor trip signal on the DAS. Completion of the implementation of this modification will be monitored under Action 4 of GDA Issue **GI-AP1000-FS-03**.

308 In my GDA Step 3 report, I noted that there is no discussion of PCI failures as a result of the reactivity insertion faults within the Westinghouse analysis. During GDA Step 4, in response to RO-AP1000-50, Westinghouse has performed analysis (Ref. 73) to demonstrate that for faults more frequent than 1×10^{-3} per year the protection can be set for each new fuel reload, to ensure that damaging conditions will not be reached without a reactor trip signal. This work has been assessed and is reported in the fuel and core assessment report (Ref. 17). This concludes that Westinghouse has taken appropriate measures to reduce the risk of PCI failures occurring for frequent fault conditions.

Methods and Assumptions

309 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling the uncontrolled RCCA bank withdrawal fault, Westinghouse has made the following assumptions to ensure a robust and conservative assessment.

- Nominal initial conditions are assumed in accordance with the revised thermal design procedure. Uncertainties in the initial conditions are instead included in the DNBR limit.
- The reactor trip on high neutron flux is assumed to be actuated at a conservative value of 118% of nominal full power.
- A bounding range of reactivity insertion rates is assumed.
- Studies are performed assuming both the maximum and minimum moderator density coefficient.
- When the minimum moderator density coefficient is assumed, its value is taken to be zero and the minimum Doppler coefficient and kinetic coefficients are assumed.
- When the maximum moderator density coefficient is assumed, the maximum Doppler coefficient and kinetic coefficients are assumed.
- The RCCA with the greatest worth is assumed to remain stuck out of the core.
- The set-point values include instrumentation and set-point uncertainties and the maximum time delays are assumed within the analysis.

310 The Westinghouse analyses use the LOFTRAN, FACTRAN and VIPRE-01 computer codes to model these uncontrolled RCCA bank withdrawal faults. The assessment of VIPRE-01 code against the validity of assurance SAPs FA.18 to FA.22 is reported in the fuel and core assessment (Ref. 17). The general assessment of the LOFTRAN code is reported in Section 4.3.4. The LOFTRAN code uses a point kinetics model for the analysis of these faults.

311 These methods and assumptions represent a standard approach to the design basis analysis of such faults and are comparable to those applied in the Sizewell B analysis.

Taken together, these assumptions are judged to provide a bounding assessment, thereby meeting the requirements of SAP FA.7.

Transient Analysis

312 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. In practice, for the faults considered in this section, the aim of Westinghouse is to demonstrate that this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB. To confirm that these objectives have been achieved, the results of design basis analysis of Westinghouse for these faults are reviewed.

313 The analysis results of Westinghouse are summarised in Figs 15.4.2-15 and 15.4.2-16 which presents the minimum DNBR as a function of reactivity insertion rate for the 100% and 60% power cases respectively. Sensitivity studies are presented for both the minimum and the maximum reactivity feedback coefficient. The results suggest that there is always an effective trip parameter to ensure adequate margin to DNB for the entire range of reactivity insertion rates.

314 When the same minimum feedback cases were analysed for Sizewell B, results were presented for 100% and 80% power operation because sensitivity studies demonstrated that the 80% power case is the most bounding in terms of DNB. All the trip parameters for Sizewell B that are claimed were presented (Ref. 46). The only reactor trip parameters plotted by Westinghouse on Figure 15.4.2-15 are the high flux and overtemperature ΔT trips. Since no other reactor trip parameters are presented it is impossible to verify whether these signals are functionally capable of protecting against the fault when assessed against the requirements of SAPs ESS.2, ESS.4 and ESS.6. In my judgement it is unlikely that any of these reactor trip signals will be able to provide effective protection against DNB over the whole range of reactivity insertions speeds that is being considered. The figure shows that even the trip parameters that are plotted are unable to provide effective protection over the full range of reactivity insertion speeds. For example, the trip on overtemperature ΔT is seen to be ineffective at faster insertions speeds. In contrast, the Sizewell B analysis plots all the trip parameters over the full range of insertion speeds thus demonstrating that there is always two trip parameters that provide effective protection against DNB for the full range of reactivity insertion speeds.

315 In my view, there is a need to demonstrate that diversity of protection against DNB exists for the full range of fault speeds and power levels. However, I recognise that additional protection has already been proposed. As a result, it is my judgement that the requisite additional analyses are unlikely to require any further plant modifications recognising that there is scope for reducing the conservatism in the assessment as the sequence frequency reduces. I have therefore raised Assessment Finding **AF-AP1000-FS-30** for a future licensee to provide this demonstration.

316 Westinghouse categorise the uncontrolled RCCA bank withdrawal fault as a Condition II event. As such, it is a frequent event within the traditional UK approach to design basis analysis, requiring two diverse safety systems to be provided for each safety function. In its responses to RO-AP1000-47 (Ref. 29) and RO-AP1000-51 (Ref. 47), Westinghouse has identified the following limiting fault sequences that need to be assessed to demonstrate that the AP1000 has diverse means of achieving each safety function:

- uncontrolled RCCA bank withdrawal with subsequent failure of the RCCAs to insert following the initiation of a reactor trip signal, and;
- uncontrolled RCCA bank withdrawal with failure of the PMS to initiate a reactor trip signal.

317 Westinghouse discounts the possibility of the first event on the grounds that it cannot envisage how RCCAs that have just been withdrawn from the core could fail to re-enter following reactor trip. This does not consider the fact that the main shutdown banks of the reactor are withdrawn during normal operation. In practice, I have seen analysis performed for other PWRs that shows that the ATWT due to RCCAs failing to insert is generally bounded by the ATWT event due to failure of primary protection. This is because the reactor trip signal on the primary system, which is based on fast acting flux detectors, is normally much faster acting than on the secondary protection system and so the turbine is tripped very quickly with a resulting decrease in steam flow which raises temperatures and pressures on the primary side. The temperature increase (which reduces the core power) and the rise in pressure protect against DNB such that the failure in primary protection system is probably the more demanding ATWT case to study. Nevertheless, I have raised Assessment Finding **AF-AP1000-FS-31** for a future licensee to confirm that the ATWT event due to failure for RCCAs to insert is bounded by the ATWT event due to failure in PMS to trip the reactor.

318 The results of the analysis for the failure of PMS to trip are presented in Figure 7.4-1 and 7.4-6 for full power conditions and Figure 7.4-19 for part power conditions of the response to RO-AP1000-51 (Ref. 47). The analysis claims the new high hot-leg temperature trip on the DAS (Ref. 47) and assumes what it describes as a realistic upper limit for incremental reactivity worth at hot zero power of 12 pcm/step for the grey rods or about 15 pcm/second given the maximum RCCA bank withdrawal rate of 72 steps per minute. Westinghouse notes that the axial offset bank has a higher maximum incremental worth (30 pcm/step) but is limited to a maximum withdrawal rate of 8 steps per minute (4 pcm/step). Westinghouse argues that higher rates are possible at zero and lower power over a short range of control rod travel but that they cannot be sustained. They also assume a power distribution consistent with full power operation arguing that faults starting from sub-critical or low power have to obtain full power levels to become a concern. Studies are done from 100%, 60% and 0% power. On the basis of its analysis, Westinghouse argues that fuel can be prevented from entering DNB if the hot-leg temperature trip set-point on the DAS is set at 335°C. The Westinghouse analysis suggests that the case from full power is bounding.

319 I welcome the development of this extra high hot-leg temperature reactor trip parameter on the DAS, which I judge to be a significant safety benefit. Progress with the implementation of the modification will be monitored under Action 4 of GDA Issue **GI-AP1000-FS-03**.

4.2.6.4 Assessment of RCCA Misalignment

320 RCCA misalignment covers a range of faults including:

- one or more dropped RCCAs within the same group;
- a statically misaligned RCCA, and:
- withdrawal of a single RCCA.

321 In my GDA Step 3 report (Ref. 6), I chose to sample the withdrawal of a single RCCA fault as it is Condition III event for which Westinghouse concedes there is a potential for

DNB to occur. Although a discussion of the analysis methodology and results is provided within the EDCD (Ref. 16), no detailed analysis of the results is presented for this fault. Westinghouse concedes that, depending upon the initial bank insertion and location of the withdrawn RCCA, an automatic reactor trip may not occur sufficiently fast to prevent the minimum DNBR from falling below the safety analysis limits. Westinghouse claims that overtemperature ΔT tripping will limit the number of fuel rods with a DNBR less than the safety limit to less than 5%. As this is potentially a frequent fault with an initiating frequency that could be greater than 1×10^{-3} per year, I do not consider this to represent an ALARP position. In contrast, the primary protection system for Sizewell B is fitted with additional protection for such faults. Reactor trip signals are provided for RCCA misalignment, incorrect RCCA bank movement and for the RCCA bank insertions limits being exceeded. In contrast, the AP1000 is provided with in-core detectors which might be able to protect against these faults provided they are connected to one of the reactor protection systems.

322 For this reason, during GDA Step 4, RO-AP1000-91 (Ref. 10) was raised requesting Westinghouse to consider the feasibility of connecting the in-core detectors to the reactor protection system. In its response to RO-AP1000-91 (Ref. 74), which largely relies upon the ATWT analysis performed in its response to RO-AP1000-51 (Ref. 47), Westinghouse argues that the most limiting fault in this category is the dropped RCCA fault and this is protected against by a control function that will block RCCA withdrawal if the power decreases too rapidly. This function, P-17, has been provided as a recent modification (Ref. 75) and is similar to a negative flux rate trip (as available on Sizewell B), except that the function only blocks automatic RCCA withdrawal and does not initiate a reactor trip. P-17 is triggered by a rapid reduction in neutron flux based upon signals directly from the ex-core detectors and so is claimed to be diverse from the PMS comparators or logic. Westinghouse claims that the analysis it has performed demonstrates that DNB can be avoided without the need for a reactor trip.

323 HSE-ND has not had the opportunity to assess this response in detail. Nevertheless, it is clear that the response considers only common mode failure of the PMS. It does not consider the possibility of common mode failure of the ex-core detectors. For this reason, I have raised Action 3 under GDA Issue **GI-AP1000-FS-03**, for Westinghouse to demonstrate diverse protection for this fault. Clearly, connecting the in-core detectors to the diverse protection system would potentially provide diverse protection for this function. For this reason, I have raised an additional GDA Issue **GI-AP1000-FS-04**, for Westinghouse to consider the feasibility of providing both enhanced and diverse protection to this fault by connecting the in-core detectors to a diverse protection system.

324 A related matter is that as part of the initial test programme described in Chapter 14 of the EDCD (Ref. 16), Westinghouse is proposing to perform RCCA misalignment measurements on only the first AP1000 plant to be built to confirm the performance of the in-core detectors. Given that on the UK design the in-core detectors could be part of a diverse protection system, additional bespoke testing of the in-core detectors could be necessary. For this reason, Assessment Finding **AF-AP1000-FS-32** has been raised requiring a future licensee to develop proposals to identify what testing will be necessary on the first of a kind AP1000 design in the UK.

4.2.6.5 Assessment of CVS Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant (Limiting Frequent Fault at Shutdown)

Fault Sequence Analysis

325 This section of the report considers homogeneous boron dilution faults caused by a failure of the CVS. Such faults can occur while the reactor is at power and while it is shutdown. They result in the uniform reduction of the boron concentration in the core and are classified as Condition II events. Westinghouse has treated them as design basis faults, meeting the requirements of SAPs FA.4 and FA.5.

326 Westinghouse argues that there are multiple redundancies within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met. The transient analysis studies for this event with the reactor at power focus on demonstrating that the protection system can successfully trip the reactor to avoid the fuel going into DNB; on a shutdown reactor the aim is to demonstrate that the reactor remains sub-critical.

327 For a boron dilution fault occurring at power, Westinghouse makes claims on the same protection systems as those identified for the uncontrolled RCCA withdrawal fault at power. However, additional alarms are provided to the operator based upon high RCCA insertion limits and axial flux differences to cover the case of a boron dilution event occurring with the reactor at power with the control system in operation. In such circumstances the RCCA banks can become deeply inserted and it is possible to get an adverse power distribution within the core. Upon receipt of a reactor trip signal the protection system automatically isolates the demineralisation water transfer and storage system. For faults occurring during shutdown, conditions are protected by the source-range flux-doubling signal which automatically isolates make-up flow, the make-up pump suction line, and the demineralisation water transfer and storage system.

328 During GDA Step 4, Westinghouse have confirmed in TQ-AP1000-840 (Ref. 9) that a reactor doubling-time trip signal is provided on the PMS for very low power operation. The trip signal parameter was missing from the list of trip parameters presented in Table 7.2-2 of the EDCD (Ref. 16).

Methods and Assumptions

329 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling uncontrolled boron dilution faults, Westinghouse has made the following assumptions to ensure a robust and conservative assessment.

- For faults occurring while the reactor is shutdown, a dilution flow of 39.75 m^3/hr is assumed. For faults occurring while the reactor is in start-up mode or at power, a dilution flow of 45.42 m^3/hr corresponding to the maximum letdown rate is assumed.
- A conservative estimate of the reactor coolant volume is made.
- A conservative assessment is made of the initial critical boron concentration corresponding to the minimum shutdown margin. The RCCA with the highest worth is assumed to be stuck in the fully withdrawn position.
- For the shutdown faults it is assumed that at least one RCP will be operating, or the demineralisation water isolation valves will be closed, or the RNS pumps will be operating such that the fault is prevented or the reactor coolant is well mixed.

330 These assumptions have not been assessed in detail during GDA Step 4 from a fault study perspective but they seem sensible and should result in a bounding assessment meeting the requirements of SAP FA.7.

Transient Analysis

331 The EDCD does not present the transient analysis results for these faults in detail. Nevertheless, Westinghouse argues that boron dilution faults occurring at power are very slow faults and are either bounded by the uncontrolled RCCA withdrawal at power fault or, if the reactor is on automatic control mode, can be adequately protected by the operator based upon RCCA insertion alarms. In the case of boron dilution faults occurring from shutdown conditions, Westinghouse claims the doubling time signal on the ex-core source range detectors will automatically isolate the source of the dilution.

332 Westinghouse categorises boron dilution faults as Condition II events. As such, they are regarded as frequent events, which require two diverse safety systems to be provided for each safety function. In its responses to RO-AP1000-47 (Ref. 29), RO-AP1000-51 (Ref. 47) and RO-AP1000-91 (Ref, 74), Westinghouse has identified the following limiting fault sequences that need to be assessed to demonstrate that the AP1000 has diverse means of achieving each safety function:

- boron dilution fault at power with failure of the PMS, and;
- boron dilution fault at shutdown with failure of the PMS.

333 Westinghouse argues (Ref. 47) that the first fault is bounded by the uncontrolled RCCA bank withdrawal fault at power with protection provided by the high hot-leg temperature trip on the DAS. In the case of the reactor being on automatic control mode, then the RCCAs will become deeply inserted. However, as the AP1000 is provided with grey automatic RCCAs for reactivity control (although it does have black RCCAs for axial flux distortion control), the distorted power distribution that can occur is not considered to be a concern with regard to DNB. If the operator does not respond to alarms, the RCCA would become fully inserted and the fault would then respond like the manual case.

334 Westinghouse argues (Ref. 74) that for the boron dilution fault at shutdown the source range detectors give an independent audio alarm that does not require PMS processing. Failure of the ex-core detectors would result in loss of this continuous audio count rate signal. This latter point seems to assume a particular failure mode for the ex-core detectors rather than more subtle common mode failure such as a calibration error. For this reason, I have raised Action 7 of GDA Issue **GI-AP1000-FS-03** for Westinghouse to demonstrate a diverse means of protection for boron dilution events occurring from shutdown conditions. As the in-core detectors could also be of benefit for this fault if they were connected to a diverse protection system, this fault is also relevant to GDA Issue **GI-AP1000-FS-04**.

4.2.6.6 Assessment of Inadvertent Misloading

335 In my GDA Step 3 report (Ref. 6), I noted that the issue of inadvertent loading of a large number of fuel assemblies will need to be explored following the operational incident at Dampierre-4 (Ref. 76) in France. An assessment of this fault has been performed in GDA Step 4 but it is reported in the fuel and core assessment (Ref. 17)

4.2.6.7 Assessment of Rod Ejection Faults

336 RCCA ejection accidents are defined as the mechanical failure of the pressure housing of a RCCA drive mechanism resulting in the ejection of an RCCA and drive shaft. The consequences of this mechanical failure are a rapid positive reactivity insertion together with an adverse core power distribution with the potential to lead to localised fuel rod damage. The transient analysis aims to demonstrate that the inherent characteristics of the reactor core coupled with the protection system can control the fault quickly enough to avoid significant fuel damage. The fault is primarily a race between the rate of increase in the stored energy in the affected fuel rods as the RCCA is ejected and the Doppler feedback coefficient which counteracts the reactivity insertion.

337 In my GDA Step 3 report (Ref. 6), the Westinghouse analysis methods applied to this fault (Ref. 77) and reported in the EDCD (Ref. 16) were compared against similar analysis performed for Sizewell B (Ref. 78). I noted that the results gave confidence in the AP1000 analysis suggesting that the 1D analysis methods used by Westinghouse were conservative, and that therefore the RCCA bank insertion limits for AP1000 were adequate. I also noted that the results were largely governed by the design of the fuel assemblies and were not overly sensitive to the operating conditions of the reactor core. However, I also noted that the Radial Averaged Peak Fuel Enthalpy (RAPFE) safety limit, against which the peak fuel enthalpy is assessed, was undergoing revision by Westinghouse: it was likely that the fault analysis would need to move to 3-D methods to accommodate these changes. During GDA Step 4, Westinghouse has moved over to a 3-D analysis making the analysis reported in the EDCD (Ref. 16) obsolete. The revised analysis (Ref. 79) has been assessed during GDA Step 4 and is reported in the fuel and core design assessment report (Ref. 17). This concludes that the adoption of this detailed assessment methodology provides a more realistic representation of the likely core response to this fault than previously, while still retaining substantial conservatism.

4.2.6.8 Consequential Failures

338 The consequential failure of a PSV failing to reseat following reactivity and adverse power distribution faults and resulting in a consequential LOCA has already been discussed in Section 4.2.3 above.

4.2.6.9 Controlled State to Safe Shutdown State

339 In its response to RO-AP1000-52 (Ref. 35), Westinghouse's treatment of reactivity and adverse power distribution faults is identical to that for the increase in heat removal faults discussed in Section 4.2.2 above. Essentially, Westinghouse argues that reactivity and adverse power distribution faults fall into the intact circuit fault group.

340 As with the case of increase of heat removal faults, the Westinghouse response is not sufficiently detailed enough with regard to each specific fault type within this class to provide an adequate final safety case. It should be noted that a boron dilution fault occurring at power will be the most limiting fault in terms of the long-term control of reactivity function (i.e. after the initial reactor trip) for all intact circuit faults. This is because the core boron concentration will be in a significantly depleted condition. Hence, Assessment Finding **AF-AP1000-FS-16** is seen to be also applicable to these faults.

4.2.6.10 Radiological Consequence Assessment

341 SAPs FA.3 and FA.7 require that a conservative radiological consequence assessment should be performed for each design basis fault sequence that can lead to the release of

radioactive material. As discussed previously in Sections 4.2.2.8, 4.2.3.8 and 4.2.5.5 above, Westinghouse has had to revise its radiological consequence analysis in response to RO-AP1000-48. A detailed review of the radiological consequence methodology applied by Westinghouse in its response to RO-AP1000-48 is presented in Section 4.6 below. The conclusion of this review is that in general the methodology appears sensible and conservative but that in some areas further justification will be required as part of the site licensing process. On this basis, it is my judgement that the methodology presented in the RO-AP1000-48 response (Ref. 50) is broadly appropriate for this preliminary Step 4 GDA assessment of individual faults against Target 4 in the HSE SAPs.

342 The response to RO-AP1000-48 (Ref. 50) argues that most of these reactivity and power distribution faults can be bounded by the activity release in the loss of off-site power fault. This is also a Condition II event. Westinghouse argues that this sequence is bounding even though the SG relief valves are assumed to operate normally because a stuck open relief valve on the AP1000 plant results in the affected SG being isolated. In contrast, if the safety relief valves operate normally, they continue to open and close for an extended period. This claim has not been assessed during Step 4 but can be reviewed as part of the closure of Action 1 of GDA Issue **GI-AP1000-FS-02**. The predicted radiological release from the loss of off-site power fault is 0.05 mSv which comfortably meets the BSL limit of Target 4.

343 For two cases, the single RCCA withdrawal fault at power and the RCCA ejection fault, Westinghouse has adopted a different approach. The single RCCA withdrawal fault is assumed to result in the failure of less than 5% of the fuel in the core. The primary circuit remains intact but a small SG leak is assumed which results in release to the environment. It is bounded by the 2.8 mSv release associated with a locked rotor fault. The RCCA ejection fault is assumed to result in the failure of less than 10% of the core. Since the initiating event is caused by a small break in the primary circuit, there is a small release to the containment from where it could reach the environment via containment leakage. This is predicted to result in a 5.5 mSv release. As a Condition IV event this meets the requirements of SAP Target 4.

4.2.6.11 Findings

344 I welcome the decision of Westinghouse to implement a modification to provide a high hot-leg temperature trip signal on the DAS. In my judgement, this modification represents a significant safety improvement. Progress with this modification will be monitored under Action 4 of the GDA Issue on functional diversity, **GI-AP1000-FS-03**. However, I consider there is still a need to demonstrate diverse protection against RCCA misalignment faults, including dropped RCCA faults, and boron dilution faults from shutdown conditions. For this reason, Actions 3 and 7 of GDA Issue **GI-AP1000-FS-03** have been raised requiring Westinghouse to provide such demonstrations. Potentially, the AP1000 in-core detectors could provide additional protection against these faults. For this reason, GDA Issue **GI-AP1000-FS-04** has been raised requiring Westinghouse to review the feasibility of connecting these in-core detectors to a diverse protection system (DAS or PLS).

345 A number of assessment findings have been raised. In general, these are items requiring further analysis or support from commissioning tests rather than fundamental issues with the design and in my judgement they can be closed out as part of the site licensing process.

4.2.7 Increase in Reactor Coolant Inventory Faults

4.2.7.1 Summary of Westinghouse's Safety Case

346 Faults in this category cause an increase in the inventory of the primary circuit leading to a rise in the pressuriser level; this potentially challenges the integrity of the primary circuit should the pressuriser become water-solid. Following successful reactor trip, it is necessary to ensure that adequate post-trip cooling is provided to avoid flooding through the pressuriser since failure to do so will challenge the integrity of the primary circuit. Faults in this category, together with the heat-up faults discussed above, effectively determine the minimum heat removal requirements of the PRHR heat exchanger and limit the maximum size of the CMTs for a given pressuriser size. Given the high pressures possible in the primary circuit, there is the possibility that the primary safety relief valves will lift and fail to reseat. Failure of a relief valve to reseat will result in a consequential LOCA.

347 The basis of Westinghouse's safety case is that it has reviewed a number of postulated events that it considers to be within the design basis of the plant and that could result in an increase in the reactor coolant inventory. For those cases which it considers to be limiting, it has performed detailed analyses and demonstrated that, even for the most bounding faults, the reactor protection system is able to trip the reactor and initiate adequate post trip cooling using the PRHR heat exchanger, so avoiding overfilling the pressuriser and over pressurising the primary circuit.

348 In performing the transient analysis, Westinghouse has undertaken sensitivity studies on the effects of the availability of offsite power following reactor trip, since this would result in the tripping of the RCPs. It also claims to have modelled the worst single failure in the reactor engineered safety features: this is that one of the discharge valves on the PRHR fails to open. On the basis of the analysis presented, Westinghouse has concluded that the PRHR provides adequate levels of post-trip cooling such that the pressuriser never becomes water-solid threatening the structural integrity of the primary circuit.

4.2.7.2 Assessment Overview

349 Westinghouse has considered the following faults within this category that it considers to be limiting and which are presented within the EDCD:

- inadvertent operation of the CMTs during power operation, and;
- CVS malfunction that increases reactor coolant inventory.

350 These are both Condition II events according to Westinghouse's classification scheme. I have chosen to sample both of these faults. Westinghouse regards the first fault as the most bounding fault in this fault category and it is a fault that is unique to the AP1000.

4.2.7.3 Assessment of Inadvertent Operation of the Core Makeup Tanks

Fault Sequence Analysis

351 Westinghouse has identified that the inadvertent operation of the CMTs at power is a Condition II event and so it is treated as a design basis event, meeting the requirements of SAPs FA.4 and FA.5. Westinghouse has identified what it considers to be the most onerous single failure (failure of one discharge valve on the PRHR). Clearly, the failure of a PRHR discharge valve to open will reduce the rate that the PRHR is able to remove decay heat from the primary circuit such that the claim that this is the bounding single failure appears plausible. The protection signals that are claimed are all based upon

2-out-of-4 voting logic. However, the pressuriser safety relief valves are predicted to lift and there is no discussion about the implications of one of these valves failing to reseat on demand as a potential candidate for the single failure. This consequential failure is discussed further in Section 4.2.7.5 below.

352 The analysis modelling the inadvertent operation of the CMTs assumes that only one of the tanks is initiated. Westinghouse's justification for only considering one CMT spuriously operating is that operation of both CMTs would only occur following a spurious safeguard ("S") signal which would also trip the reactor. Operation of a single CMT allows operation at power to continue making the fault more onerous. The evidence supporting this claim is that there are no failure modes in the protection system which can result in spurious operation of both CMTs at power: this has been reviewed in GDA Step 4 and is discussed in Section 4.2.10 on control and protection system faults.

Transient Analysis

353 The pressuriser water volume transient for inadvertent operation of the CMTs is presented in Fig 15.5.1-5 of the EDCD (Ref. 16). The water level is seen to rise during the transient up to levels comparable with the loss of normal feed and feedline break faults considered earlier. It is this transient, together with those presented for the feed system faults, that provides the sizing constraints for the minimum heat removal capacity of the PRHR and the maximum size of the CMTs for a given size of pressuriser.

354 As a frequent event, it needs to be treated within the traditional UK approach to design basis analysis which requires two diverse safety systems to be provided for each safety function. In its response to RO-AP1000-51 (Ref. 47), Westinghouse argues that inadvertent operation of the CMT involves tripping the RCPs and opening of the CMT discharge valves. Should a RCP trip not to occur, then the pressure gradients will prevent flow through the CMT since a check valve in the CMT discharge line prevents reverse flow. If the RCPs trip, then the ATWT case without PMS is claimed by Westinghouse to be bounded by the complete loss of forced coolant flow case discussed above. The reactor will be tripped by the high hot-leg temperature reactor trip signal on the DAS which will also actuate the PRHR and the PCS. I agree with these arguments. Clearly, if an extra RCP underspeed trip signal is provided on the DAS in response to Action 5 of GDA Issue **GI-AP1000-FS-03** this may also be of benefit for this fault as well.

4.2.7.4 Assessment of CVS Malfunction that Increases Reactor Coolant Inventory

Fault Sequence Analysis

355 Westinghouse has identified that the inadvertent operation of the CVS at power is a Condition II event and so it is treated as a design basis event meeting the requirements of SAPs FA.4 and FA.5. Westinghouse has identified what it considers to be the most onerous single failure (failure of one discharge valve on the PRHR). Clearly, the failure of a PRHR discharge valve to open will reduce the rate that the PRHR is able to remove decay heat from the primary circuit such that the claim that this is the bounding single failure appears reasonable. Thus the single failure criteria of SAPs FA.6, EDR.2 and EDR.4 are met. The protection signals that are claimed are all based upon 2-out-of-4 voting logic.

356 During normal operating conditions, the PMS will detect the fault on high-2 pressuriser level and the CVS will be isolated without need for a reactor trip. The pressuriser safety relief valves are not predicted to lift. However, if the CVS injects highly borated water while the reactor is under manual control, the fault could cause a cooldown of the RCS at

some points in the fuel cycle. This will result in either a low T_{cold} signal or a low steamline pressure 'S' signal being generated, tripping the reactor. Since only the PRHR is available to remove decay heat, the PSVs are predicted to lift. However, although there is an increase in the RCS inventory, the transient analysis predicts that the pressuriser will not overfill.

357 As a frequent event this fault needs to be treated within the traditional UK approach to design basis analysis which requires two diverse safety systems to be provided for each safety function. In its response to RO-AP1000-51 (Ref. 47), Westinghouse argues that in terms of the RCS overpressure safety limit, inadvertent operation of the CVS is bounded by the loss of ac ATWT event, which is itself bounded by the loss of normal feedwater fault ATWT event discussed in Section 4.2.3.5 above. I accept these arguments.

4.2.7.5 Consequential Failures

358 The consequential failure of a PSV failing to reseat following an increase in reactor coolant inventory fault and resulting in a consequential LOCA fault is discussed in Section 4.2.3 above.

4.2.7.6 Controlled State to Safe Shutdown State

359 In its response to RO-AP1000-52 (Ref. 35), Westinghouse's treatment of increase in reactor coolant inventory faults is identical to that for the decrease in heat removal faults discussed in the Section 4.2.3.6 above. Essentially, Westinghouse is arguing that increase in reactor coolant inventory faults fall into the intact circuit fault group. I agree with this conclusion.

4.2.7.7 Radiological Consequence Assessment

360 In its response to RO-AP1000-48 (Ref. 50), Westinghouse argues that faults in this category are adequately protected against without the need for a reactor trip and that therefore there is no release of activity to the environment such that the requirements of Target 4 of the SAPs are automatically met. While this is true for many of the initiating events bounded by these faults, the EDCD (Ref. 16) identifies some initiating events where a reactor trip is required. However, without additional failures these faults will remain intact circuit faults and so releases should be bounded by the loss of off-site power fault discussed in Section 4.2.5.5 above, so meeting the requirements of Target 4. As part of Assessment Finding **AF-AP1000-FS-46** discussed in Section 4.6 below, a future licensee will be required to confirm that the releases do meet the requirements.

4.2.7.8 Findings

361 I agree with Westinghouse that the consequences of these faults are adequately protected against.

4.2.8 Decrease in Reactor Coolant Inventory Faults

362 The assessment of Westinghouse's safety case for decrease in reactor coolant inventory faults has been split into three areas:

- SGTR;
- SBLOCA, and;

- LBLOCA.

363 Breaks in instrument lines that penetrate the containment have not been assessed for Step 4 of the GDA.

4.2.8.1 Summary of Westinghouse's Safety Case for SGTR

364 The design basis fault considered in Chapter 15 of the EDCD is the complete severance of a single SG tube from power. The fault is categorised by Westinghouse as a Condition IV event (i.e. a fault that is not expected to take place during the life of the plant but is postulated because the consequences include the potential for the release of significant amounts of radioactive material). The frequency attributed to the fault in response to RO-AP1000-46 (Ref. 37) is 4×10^{-3} per year which defines it as a frequent fault (although the response to RO-AP1000-47 (Ref. 29) only considers it as a "cliff-edge" frequent fault).

365 The accident leads to an increase in contamination of the secondary system due to leakage of radioactive coolant from the primary coolant system. In the event of the non-safety grade condenser steam dump being unavailable (either due to a fault or a coincident loss of power), a discharge of radioactive steam is possible via the SG PORVs or the safety valves.

366 Westinghouse claims in the EDCD that complete severance is conservative because the SG tube material (Alloy 690) is a corrosion-resistant and ductile material. Water chemistry on both the primary and secondary side will be controlled to minimise corrosion. The Model Delta-125 steam generator is designed to minimise the potential for mechanical or flow-induced vibration. The more probable mode of tube failure is stated to be one or more smaller leaks of undetermined origin. It is intended that activity in the secondary side will be subject to continual surveillance and an accumulation of such leaks, which exceeds the limits established in the Technical Specification, will not be permitted during operation.

367 The AP1000 design provides automatic protective actions to mitigate the consequences of a SGTR. These actions result in the automatic cool-down and depressurisation of the RCS, termination of the break flow and release of steam to atmosphere, and long-term maintenance of stable conditions in the RCS. Westinghouse has undertaken design basis analysis to demonstrate that these protection systems prevent SG overfill and constrain the off-site radiation doses (by limiting the active steam release) to allowable US NRC guideline values. This design basis event should not result in any DNB or any fuel failures unlike other depressurisation events that are associated with larger but less frequent breaches. The provision the PRHR to remove decay heat is a significant design feature which means that the SGs can be isolated following a SGTR fault. This diverse means of cooling is a major advantage for the AP1000 design in dealing with SGTR faults.

368 In addition to the automatic protection, the operator is provided with sufficient indications and controls to mitigate of the consequences of an SGTR more rapidly. The design basis transient analysis in the EDCD is based upon the automatic actions for a reactor operating at full power prior to the fault. No operator actions are modelled.

4.2.8.2 Assessment of SGTR Faults

Overview

369 I have assessed the SGTR analysis presented in the EDCD and its supporting references principally against the requirements of SAPs FA.1 to FA.8 and FA.17 to FA.22. I also

commissioned AMEC to review the same references and perform some independent confirmatory analysis.

Fault Sequence Analysis

370 The sequence of events following a SGTR is clearly described in the EDCD for both automatic and operator recovery actions in accordance with SAP FA.6. In the design basis analysis, the reactor is assumed to trip and lose off-site power concurrently with the rupture of the tube. After the reactor trip, the secondary side pressure increases rapidly until the SG PORVs (and safety valves if their set-point is reached) lift to dissipate the energy. The leak flow through the tube rupture depletes the primary inventory such that the low pressuriser level "S", CMT and PRHR actuation signals are reached. Actuating the PRHR heat exchanger transfers core decay heat to the IRWST and initiates a cool-down (and consequential depressurisation) of the RCS. The CMTs provide borated make-up water via recirculation directly to the reactor vessel down-comer to maintain the reactor coolant inventory. They also contribute to decay heat removal. The CMTs do not enter drain-down mode and ADS depressurisation is not actuated for this fault. Eventually the CVS pumps and pressuriser heaters are isolated to minimise the repressurisation of the primary system. This allows the primary pressure to fall and equilibrate with the secondary pressure, effectively terminating the primary to secondary break flow.

371 The AP1000 SGTR design basis safety case effectively contains two significant claims: (i) the maximum amount of activity released via steam to atmosphere is within acceptable limits; and (ii) the SGs will not overfill, thus avoiding the radiological consequences of a release of liquid to atmosphere via secondary-side relief valves in addition to the steam releases (there are also concerns about the structural integrity of the main steamlines due to the accumulation of water). Two slightly different bounding fault sequences are considered to demonstrate that these two claims are met with different boundary conditions and single-failure assumptions. The assumptions made for the case maximising the steam release are clearly presented in the EDCD. The margin to overfill case is not given the same prominence in the EDCD but its supporting references are equally clear about what has been assumed.

372 Both sequences claim the Class A1 safety systems and make conservative assumptions on the performance of the active safety systems and operational systems, in accordance with SAP FA.6 (specifically that they do not operate or they operate in such way to maximise the consequences of the fault). The choices of the worst single failure seem sensible. However their selection appears to have originated from work pre-dating the AP1000. These choices need further substantiation and consideration needs to be given to whether changes in radiological consequences analysis methodology can change previously limiting assumptions (see Section 4.6).

373 The EDCD does not consider multiple tube ruptures. While multiple tube ruptures are expected to be less likely than a single tube rupture, the SAP FA.4 (Ref. 4) sets the expectation that faults with initiating event frequencies down to 1×10^{-5} per year should be considered within the design basis. Therefore, even if the frequency of a multiple tube rupture is two orders of magnitude less likely than a single tube rupture, it could still be a candidate for design basis analysis. In response to TQ-AP1000-441 (Ref. 9), Westinghouse has undertaken transient analysis to investigate multiple (and partial tube ruptures) in the AP1000. Westinghouse has stated that it intends to report this analysis in the PCSR, which will be assessed under the Cross-cutting topic area assessment GDA Issue **GI-AP1000-CC-02** (Ref. 144). The results of the analysis presented in the TQ response are discussed further below.

374 As a frequent event, the SGTR fault needs to be treated within the traditional UK approach to design-basis analysis which requires two diverse safety systems to be provided for each safety function. In its response to RO-AP1000-47 (Ref. 29), Westinghouse argues that the SGTR fault is bounded by the frequent SBLOCA fault considered in Section 4.2.8.5 below. In my opinion, while this statement is true in terms of the fuel cooling function (since SGTR faults are very small LOCA for which the ADS blowdown function is not required for the primary means of protection), this does not consider the fact that design-basis SGTR faults result in containment by-pass. Therefore there is potential for the radiological release to be more onerous than the SBLOCA fault depending upon the common mode failure considered. In particular, consideration has to be given to failure to isolate the MSIV and any other potential radiological leak paths.

375 My judgement is that the AP1000 is probably better protected than Sizewell B with regard to SGTR faults and that it is therefore unlikely that any modifications will be necessary in this respect. Nevertheless, I have raised an Assessment Finding, **AF-AP1000-FS-33**, for a future licensee to confirm that following the common-mode failure of any one safety system that fulfils a safety function role for SGTR faults there is either a diverse means of protection or that the radiological consequences are ALARP and meet the requirements of Target 4 of the SAPs.

Methods and Assumptions

376 Westinghouse has used the LOFTTR2 computer code to analyse the plant response following a SGTR until primary-to-secondary break flow is terminated. This is a specialised version of the LOFTRAN code, modified to include an enhanced steam generator secondary side model and a tube rupture break flow model. Both LOFTRAN and LOFTTR2 were modified to model AP600 passive features, notably the passive residual heat removal system and the CMTs. These changes are reported in an AP600 applicability report (Ref. 49). Included within the reference are US NRC's comments and questions on the changes. Westinghouse's formal responses are also recorded. The codes do not have an explicit detailed model of the ADS as Westinghouse only use the LOFTRAN codes to model non-LOCA faults (and SGTR faults) where the ADS is not claimed as a safety feature.

377 Westinghouse has provided justification for the use of the LOFTRAN code developed for AP600 to perform analysis of the AP1000 (Ref. 52). It concludes that no new phenomena have been identified for AP1000 when compared to AP600, and the test database that supported the code validation is applicable to AP1000. In addition, Westinghouse claims that assessments have shown that the AP1000 passive safety systems operate in the same way as the AP600, and that large margins to the regulatory limits exist for the transient events analysed.

378 While LOFTRAN and LOFTTR2 are old codes and no longer represent the 'state-of-the-art', both the original codes and updated versions (to include passive features) have been subject to verification and validation. They have also been reviewed and certified by US NRC. The response of the AP600 plant passive safeguard features was based on a number of tests (SPES-1 natural circulation tests, PRHR component tests, CMT component tests, SPES-2 steam generator tube rupture and steam line break tests, see Ref. 49). While modern codes may be more powerful and flexible, there is no fundamental reason why the predictions made by LOFTTR2 should be invalid providing the transient modelled is covered by the physics and validation of the code.

379 My assessment of the LOFTRAN code and its code variants against SAPs FA.17 to FA.22 is presented in Section 4.3.4 below. However I am generally satisfied with their

appropriateness for use in SGTR design basis fault analysis in accordance with SAP FA.7. As I have already commented, I consider the experimental testing used to validate the modelling on the passive systems to have been performed to a very high standard.

380 To calculate the mass release data for radiological consequences calculations, the SGTRDOS code is used to access the LOFTTR2 output and perform the necessary calculations to determine the primary to secondary break flow and the secondary-side steam and feedwater flows from the initiation of the event to the time of leakage termination. This relatively simple code has been part of Westinghouse's standard SGTR methodology for many years and has not been assessed in detail.

Transient Analysis

381 Two parallel sets of analyses are undertaken by Westinghouse (Ref. 80) for the design basis fault with different assumptions, including different single-failure considerations. The main calculation, which is presented in the EDCD, aims to maximise the mass of steam released to provide input to a conservative dose calculation for the fault. The second calculation, which is not presented in the EDCD, makes assumptions that maximise the mass of water retained in the ruptured SG to demonstrate that there is a margin to overfill. It states that there is a margin of over 400 ft^3 (over 11 m^3) until the SG overfills. As presented, the transient analysis does appear to support the safety claims made in the EDCD.

382 However, I do have concerns about the adequacy of the EDCD analysis to accurately represent the AP1000 design proposed for GDA. The analysis is approximately 10 years old and reflects the AP1000 design at that time. Westinghouse's SGTR methodology and LOFTRAN codes are essentially unchanged since the original analysis was undertaken. Minor revisions have been made to the computer codes over time (appropriately) and not all will be directly linked to a specific design change (some will be e.g. error corrections, code improvements and bug fixing). However the issue is not restricted to this type of small changes to the computer codes. The EDCD supporting reference (Rev 0 of Ref. 82) identifies that it has used "LOFTRAN base deck Rev 1 (2001)". This input deck is characterised in the Ref. 82 has having many open items (outstanding issues) with provisional data values and a number of AP600 design parameters. Therefore, the analysis presented in the EDCD inevitably does not match the UK GDA Design Reference Point.

383 During GDA, Westinghouse also provided to HSE-ND an updated version (Rev 1) of Ref. 82. This used "LOFTRAN base deck Rev 3 (2007)". Multiple parameters are changed in this revised analysis (set points, delays, friction values etc) although the original arguments for the acceptability of the AP1000 design continue to be supported.

384 Westinghouse started the "Advanced First Core Analysis Programme" (AFCAP) in 2008. This involved the reanalysis of US DCD Chapter 15 faults (not for the EDCD submitted for GDA) with the latest computer models, incorporating many design changes implemented since the previous analysis was completed. It also assumed a revised core loading to reflect that proposed for Chinese AP1000s. SGTR faults were reanalysed again as part of this programme (Ref. 83). A new base deck, identified as "Advanced First Core LOFTRAN Base Deck (2009)" was used. This base deck is stated to be a draft revision and contains many open items. Multiple other open items are identified in the analysis.

385 It is apparent that none of the three generations of SGTR analyses have assumed all the design aspects of the GDA Design Reference Point. Therefore it is not possible for me make a positive assessment against SAP FA.17 which requires theoretical models to adequately represent the facility and site. I could make a presumption that the most recent analysis (Ref. 83) is the closest to the proposed GDA Design Reference Point. However both AMEC (see below) and I have assessed only the 2001 analysis presented in the EDCD and Rev 0 of Ref. 82: Westinghouse had not told HSE-ND at the time that the AFCAP analysis is the appropriate analysis to consider for the UK AP1000. A brief review of the AFCAP analysis presented in Ref. 83 shows that the timing of break flow termination is substantially changed from earlier work.

386 This issue is of concern for all design basis faults, not just SGTR faults. I have assessed the EDCD transient analysis, which although dated, is the formal submission to HSE-ND. The AFCAP work has not been formally submitted to replace the analysis in the EDCD and has not been assessed. Any new analysis performed for GDA Step 4 through ROs has used methodologies similar to those used in AFCAP. However the vast majority of the UK AP1000 design basis safety case is based on EDCD transient analysis.

387 I have therefore raised Action 1 of GDA Issue **GI-AP1000-FS-02**, requiring Westinghouse to demonstrate for all design basis faults (including SGTR faults) that the submitted design basis analysis is appropriate for the agreed GDA Design Reference Point and that all safety claims are supported by the analysis. If this cannot be done with pre-existing analysis, new analysis could be required. The final PCSR produced for GDA is to summarise this analysis for all design basis faults. Single-failure assumptions substantiated before the GDA Design Reference Point and extant methodologies were developed also need to be shown to be appropriate or revised accordingly.

388 Specifically related to calculation of the margin to overfill, Westinghouse has identified a design change (APP-GW-GEE-1294, Ref. 62) that it wishes to be included within the UK Design Reference Point. Westinghouse has established that without a modification to the SFW isolation set-point on the SG narrow range it is not possible to show a margin to overfill for a design basis SGTR fault, despite what is stated in the EDCD and the supporting calc note (Ref. 82). Westinghouse has undertaken new analysis incorporating this change but this is not referenced in the EDCD or any preliminary drafts of the PCSR (Ref. 12). It has therefore not been assessed as part of GDA Step 4. This further reinforces the requirement for Westinghouse to be very clear on what analysis it wants to be considered within GDA and then ensure it supports the claims that are being made.

389 Westinghouse's analysis of multiple tube ruptures performed in response to TQ-AP1000-441 (Ref. 9) shows that the increased break flow results in earlier actuation of the safety systems, leading to earlier break flow termination with less steam in total being released. A partial tube rupture is shown to delay the CMT and PRHR system actuation but overall it results in lower integrated break flow. Westinghouse states that this supports its claim that a double-ended guillotine break of a single tube rupture is the bounding SGTR fault. I consider the demonstration provided for the TQ adequate for GDA and I expect the PCSR to expand on this previously not discussed aspect of the safety case. However, the analysis of multiple tube ruptures is described as "scoping analysis", and no formal reference is provided for the work. I require this gap to be closed during site licensing, and as a result I have raised an Assessment Finding (**AF-AP1000-FS-34**) for formal analysis of a spectrum of tube ruptures to be considered, from less than a complete tube rupture (but exceeding the capacity CVS) to multiple tube ruptures in the same SG.

Confirmatory Analysis

390 To gain further confidence in Westinghouse's modelling of SGTR faults, I commissioned AMEC to perform confirmatory analysis of SGTR transients using an independent thermal hydraulic code and to review the single-failure assumptions. To assist in its on-going assessment and licensing of the AP1000 in the US, US NRC has developed a thermal-hydraulic model of the AP1000 for fault analysis using the TRACE code. US NRC provided HSE-ND with a copy of their AP1000 LOCA model which was passed to AMEC to allow it to start its analysis from an advanced position.

391 AMEC modified the AP1000 input deck to reflect design basis assumptions stated in the EDCD and supporting references, and also made specific changes to model SG tube ruptures. The resulting TRACE confirmatory analysis (Ref. 81) showed good general agreement with Westinghouse's EDCD analysis. The event sequence predicted by TRACE is consistent with that predicted by LOFTRAN. Sensitivity cases looking at multiple tube ruptures were also supportive of Westinghouse's arguments.

392 To develop a SGTR TRACE model and to make meaningful comparison with the EDCD results, AMEC undertook a detailed review of Westinghouse's supporting calculation notes detailing the design-basis transient analysis. AMEC found the documentation capturing the SGTR transient analysis to be a clear, accurate and detailed record of Westinghouse's work. However the reported level of detail raised further concern associated with the age and appropriateness of the EDCD analysis. AMEC also identified the requirement discussed above for single failure assumptions to be justified for the GDA design. This is because these assumptions have origins which pre-dated the current AP1000 and do not account for changes to the radiological consequences analysis methodology (see below).

Safe Shutdown State

393 All the transient analysis presented for SGTR faults stops once the flow from the primary to secondary circuits though the break is terminated. However, following break-flow termination, the reactor and nuclear steam supply system need to be brought to a safe state. The safe shutdown state is assumed to be achieved for the AP1000 following a SGTR fault when the RNS entry conditions are reached. For a frequent fault, the expectation is that this can be demonstrated with diverse safety-classified systems. This expectation was set out to Westinghouse in RO-AP1000-52 (Ref. 10).

394 In the response to RO-AP1000-52 (Ref. 35), Westinghouse has stated that the Class A1 passive systems will bring the AP1000 to an initial controlled state (the point at which the break flow is terminated) with no claim on operator actions. The sequence of events involving a reactor trip, PRHR and CMT actuation, is as described above. Ref. 35 goes on to state that the principal claimed means to reach a safe state from the controlled state is for the operator to do nothing and allow the same Class A1 passive systems to cool and depressurise the RCS to safe shutdown conditions within 36 hours.

395 The claimed diverse means to achieve the safe shutdown is passive bleed and feed, again with Class A1 systems (apart from a claim on the Class A2 DAS). The bleed is performed by manual actuation of the ADS. The feed is performed by the accumulators and gravity injection from the IRWST. In the longer term, when the IRWST reaches a low level, recirculation from the containment will be started.

396 In addition to these Class A1 systems, the RO response identifies a defence-in-depth means for achieving both the controlled state and the safe shutdown state. Although not

formally claimed in the design basis safety case, these predominately Class A2 systems are those most likely to be used to manage a fault[1]. The following actions are identified:

- RCS Cooldown – this is accomplished via steam dump from the intact SG, either via the condenser if available or to the atmosphere. For this, it is assumed that at least one SFW pump (Class A2) is running. If the intact SG is unavailable, the lengthy process with the Class A1 PHRH would have to be followed.
- RCS Depressurisation – this can be accomplished with the normal pressuriser sprays (Class 2) if at least one RCP (Class 2) is running, or with the auxiliary sprays (Class 2) with at least one CVS makeup pump (Class 2) running. If neither of these are available, the first stage ADS valves (Class A1) could be used. (Note it is not known whether Westinghouse would claim the Class 2 systems as fulfilling a Category A or B safety function).
- Ruptured SG Depressurisation – the operator has three options to bring the pressure down in the affected SG:
    1. Using Class 2 systems, backfill by reducing the RCS pressure below the ruptured SG pressure using pressuriser sprays. The pressure differential drives the secondary inventory back through the ruptured tube into the primary side. This method minimises radiological releases but the operator has to consider the adverse chemistry effects of secondary side water on the primary system components and the potential boron dilution.
    2. The SG blowdown system used in normal shutdown operations could be used. This would minimise radiological consequences and eliminate the concerns associated with introducing secondary side inventory into the primary circuit. However, it has limited storage and processing capabilities. The SG blowdown system is identified in Ref. 33 as a Class 3 system.
    3. The options above are likely to proceed slowly since they require the repeated draining of the ruptured SG through small capacity lines. In some cases it may be desirable to establish RNS cooling more quickly, e.g. to conserve SG feedwater supply. A rapid means to depressurise the ruptured SG is to dump steam either to atmosphere (Class A1) or the condenser, if available. This would result in further radiological releases.

397 It does appear that the AP1000 can reach the safe shutdown state by two diverse means, both of which use Class A1 systems. However the RO response does not demonstrate how safety criteria have been met by these assumed sequences, other than that the end state has been achieved. The radiological consequences analysis presented in response to RO-AP1000-48 assumes that there is no secondary-side activity release after break-flow termination because one of the Class 2 methods to blow down the ruptured SG will be followed. This is not consistent with the assumption of no operator actions to isolate the ruptured SG and allowing the whole system to cool and depressurise on its own. No discussion is provided on whether the radiological consequences of the bleed and feed approach are bounded by any of the other approaches. I have therefore raised an Assessment Finding, **AF-AP1000-FS-35**, for the future operator to clarify exactly what

[1] It is assumed that the operator will perform the defence-in-depth actions using the Plant Control System (PLS). While Westinghouse states (Ref. 29) that parts of the PLS will be Class A2, the operator's interface with the PLS is through the Class 3 Data Display and Processing System (DDS).

fault sequences and SSCs they are claiming for this frequent fault, and to demonstrate how all safety criteria are met down to the safe shutdown state.

398 Both Class A1 means of dealing with the SGTR fault in the end rely on the PCS as the ultimate heat sink. Westinghouse state that the PCS design incorporates diversity such that a common cause failure cannot result in its failure. The arguments for this and my assessment of this are the same as those in Section 4.2.3.5 for loss of normal feedwater faults.

399 The usual approach in design-basis analysis is to assume that operational systems (which for this case are also defence in depth Class 2 safety systems) either do not act or act is such a way to maximise the consequences of the considered sequence. The reality is that the operator would not adopt a "hands-off" approach after the controlled state had been reached, but would seek to cool the reactor to the safe shutdown state more rapidly. RO-AP1000-52 does not present a systematic discussion about how the identified fault sequences are bounding in this respect. It does consider one specific aspect associated with the defence-in-depth Class 2 actions which could be more limiting than the design basis fault sequence. If the backfill method is used, there is the potential for a large volume of unborated water to be introduced back into the primary system. Westinghouse states that if this option is selected, the operator is required to ensure that there is an adequate shutdown margin during the defence-in-depth cooldown/depressurisation actions (which are the actions that will be followed in practice). To further support this, Westinghouse has also presented a hand calculation to show that even for the limiting design-basis margin-to-overfill scenario (with failure of the SFW to throttle when the set point is reached) the average boron concentration will be above the minimum boron concentration for the considered fuel cycle. Westinghouse also states that it is confident that unborated water from the secondary side will be well mixed, making it appropriate to consider the average boron concentration. The issue of mixing of unborated water following an SGTR fault is a generic research area on PWRs for which HSE-ND is monitoring the results. However, in my opinion there is no reason for raising a finding on the AP1000 since the geometry of its loop design means that it is better placed to handle such faults when compared with the current operating fleet of PWRs.

Radiological Consequences

400 The EDCD presents radiological consequences calculated for the SGTR fault using the design basis transient analysis which maximises the steam release to the environment. However these consequences were calculated with a prescriptive methodology approved by the US NRC which is not consistent with the expectations for similar calculations in the UK. So while the presented consequences meet US NRC's criteria, it is not possible to make a meaningful comparison with Target 4 in SAPs (Ref. 4). As a result, RO-AP1000-48 (Ref. 10) was raised at the end of GDA Step 3 requiring Westinghouse to recalculate the radiological consequences predicted for design basis events (including SGTR faults) consistent with UK good practice and making an explicit comparison with Target 4.

401 More detailed discussion of the assessment of Westinghouse's revised methodology to calculate radiological consequences for design basis events is presented in Section 4.6. However the doses predicted do indicate that it should be possible with future site-specific calculations to demonstrate that the radiological consequences from the design basis SGTR event do meet Target 4 in SAPs. It is not possible at this stage to say whether Westinghouse has done everything possible to make the consequences as low as reasonably practicable. A number of the assumptions made in the analysis are rather

arbitrary and/or inconsistently applied through the analysis. More detailed justification and evidence is needed to support many of the assumptions used. Only after this is provided (in future site specific calculations) will it be possible to conclude whether, say, there is merit in reducing the allowable activity levels in the primary circuit from the limit assumed in the Ref. 50 analysis.

402 The results of the reassessment of radiological consequences (Ref. 50) give two predictions of the off-site dose to a member of the public at the site boundary. Assuming a pre-accident spike in iodine activity (caused by e.g. reactor power manoeuvres before the events) a dose of 0.53 mSv is predicted. Assuming an accident initiated iodine spike, a dose of 0.91 mSv is predicted. Both of these are below the 1 mSv BSL target set for a fault more frequent than 1 x 10^{-3} per year. To achieve this, a number of methodology changes were needed from those previously utilised by Westinghouse. Significantly, Westinghouse has also reduced the normal operation limit on primary circuit activity by a factor of 4 compared to the Technical Specification limits proposed for US plants.

403 Westinghouse's revised radiological consequences calculations have not used the transient analysis presented in the EDCD which was originally provided with the aim to maximise the mass of steam released to provide input to a conservative dose calculation. Instead Ref. 50 has used more recent (but equivalent) analysis undertaken for the AFCAP to facilitate operations at the first Chinese AP1000 to come on-line. This means that the current safety case is a hybrid of two sets of analyses for the same fault, one demonstrating that thermal-hydraulic limits are met, and another used to demonstrate that the radiological consequences are acceptable. Depending on the outcome of Action 1 of **GI-AP1000-FS-02** and the demonstration of the appropriateness of any particular set of SGTR analyses, this less than elegant position may be acceptable for GDA. However, ultimately for site licensing, a clearer linkage and consistency between the design basis transient analysis and radiological consequences analysis is expected.

404 As already stated, the fault sequence assumed in the radiological consequences is not the same as that assumed in the RO-AP1000-52 response for either the principal or the diverse fault sequences that show that the safe shutdown state can be reached. This is captured in Assessment Finding **AF-AP1000-FS-35**.

4.2.8.3 Findings for SGTR

405 The claimed ability of the AP1000 design to avoid overfilling the SGs using only automatic protection systems is a significant safety improvement on earlier PWRs.

406 An Assessment Finding, **AF-AP1000-FS-33,** has been raised for a future operator to demonstrate that for the frequent SGTR fault a diverse means of protection is provided for each safety function or that the radiological release is ALARP and meets Target 4 of the SAPs.

407 An Assessment Finding, **AF-AP1000-FS-34**, has been raised for a future operator to assess a spectrum of SG tube ruptures greater than the capacity of the CVS to compensate for to demonstrate Westinghouse's assertion that a single double-ended guillotine tube rupture is bounding.

408 An Assessment Finding, **AF-AP1000-FS-35**, has also been raised for the future operator to clarify exactly what fault sequences and SSCs they are claiming for this frequent fault, and demonstrate how all safety criteria are met down to the safe shutdown state.

409 SGTR faults need to be considered in Action 1 of GDA Issue **GI-AP1000-FS-02** for Westinghouse to demonstrate for all design basis faults that the submitted design basis analysis is appropriate for the agreed GDA Design Reference Point and that all safety

claims are supported by the analysis. This needs to include a review of the single failure assumptions which were established considering earlier designs, without reference to assumptions made in the radiological consequences analysis proposed for the UK (see Section 4.6).

4.2.8.4 Summary of Westinghouse's Safety Case for SBLOCA

410 A SBLOCA is defined in the EDCD as a rupture of the reactor coolant pressure boundary with a total cross-sectional area less than 0.09 m^2 (1.0 ft^2). The at-power fault is classified as a Condition III event. Four types of SBLOCA are considered[1]:

- Inadvertent ADS operation.
- 2-inch (50.8 mm) break in a cold-leg with CMT balance line connections.
- Double-ended rupture of the direct vessel injection line.
- 10-inch (254 mm) cold-leg break.

411 The Class A1 passive safety features of the AP1000 are claimed to prevent or minimise the core being uncovered during these SBLOCAs. The design approach is to depressurise the RCS if the break or leak is greater than the capability of the CMTs at full reactor pressure and / or if the CVS make-up system fails to perform (the CVS is not claimed to perform a safety function).

412 A reactor trip and the initiation of the PXS are actuated by the pressuriser low-pressure set-point being reached. The CMTs are the first to provide make-up in the form of cold borated water. The gravity head of the colder water provides injection at the reactor coolant pressure. Once sufficient RCS depressurisation has occurred, either as a result of the LOCA or of the actuation of the ADS, the pressurised accumulators provide additional borated water to the RCS. The IRWST provides long-term cooling when the RCS pressure reduces to a level close to that of the containment pressure. For this to occur for a SBLOCA, the ADS valves need to be actuated. The isolation valve on the PRHR system opens following the generation of the "S" signal that initiates the CMTs.

413 The SBLOCA faults have been assessed using the Westinghouse code NOTRUMP. The code originates from the early 1980's, predating passive PWR safety features. The version used for the AP1000 SBLOCA was updated and validated against applicable AP600 passive plant data (Ref. 90). Justification has been provided (Ref. 52) for the appropriateness of using the AP600 version of the NOTRUMP code for the AP1000 analysis.

414 Westinghouse's analysis shows that for all but the 10-inch cold-leg break fault, the core remains covered and therefore there is no core heat-up as a result of a SBLOCA. In the 10-inch cold-leg break fault, fluid is drawn from the bottom of the core and insufficient liquid remains in the core and the upper plenum to sustain the mixture level. The mixture level falls to a minimum then starts to recover as the accumulator flows enter the down-comer. The analysis shows that during this period, a portion of the core could dry out. Using an adiabatic heat up calculation with conservative assumptions, Westinghouse has estimated a peak clad temperature of approximately 743°C. The EDCD states that this temperature demonstrates a significant margin to the safety limit of 1204°C.

[1] Note the PSA considers different break sizes, and uses definitions of small and medium breaks which would all be considered SBLOCA in the EDCD definition. It is believed the PCSR (Ref. 13) is moving to this alternative definition.

415 Chapter 15 of the EDCD presents specific analysis of the consequences immediately following the inadvertent operation of the one of the ADS Stage-1 to 3 valves or the inadvertent opening of a PSV. Shortly after the initiating events, these faults cause a reactor trip from either overtemperature ΔT or pressuriser low-pressure protection system signals. Transient analysis is presented to show that an overtemperature ΔT reactor protection signal provides adequate protection for the faults and that the DNBR remains above the design limit during the early part of the transient (tens of seconds). The ADS valve fault is classified as a Condition III event in the EDCD while the PSV fault is a classified as a Condition II event in the EDCD.

416 Transient analysis is presented in the EDCD for an open PSV and for two open ADS Stage-1 valves. The severity of the event is presented as a combination of the effective valve area and the opening time. The effective area of two ADS Stage-1 valves is greater than that of a single PSV and is therefore presented as a bounding case in the EDCD. However the opening time of a PSV is quicker (assumed to fully open at the start of the transient) than the ADS valves and is therefore presented as separate case.

417 The effective flow area of a Stage-1 valve is stated in the EDCD to be 7 in^2 while the effective flow area of a Stage-2 and Stage-3 vales is 26 in^2. In the supporting calculation note (Ref. 88) Westinghouse has shown that the slower opening times of the Stage 2 and 3 valves means that despite the larger area, the consequences (margin to DNB) of a single Stage-2 or 3 valve opening are bounded by those predicted for two ADS Stage-1 valves opening, and therefore Westinghouse has chosen not to present the analysis in the EDCD for the former cases.

418 The LOFTRAN code has been used to model this initial period of the plant system transient and the FRACTRAN code is used to calculate the core heat flux using the LOFTRAN output. Finally the VIPRE-01 code is used to calculate DNBR values that are less than the safety analysis limit. Long-term analysis of a non-isolable stuck-open ADS valve or pressuriser safety valve (i.e. the ability to keep the core covered and prevent fuel clad heat-up via safety injection) is demonstrated by the main SBLOCA analysis.

419 Chapter 15 of EDCD considers failures of small lines carrying coolant outside of containment. No detailed transient analysis is presented. Instead the results of radiological consequences analysis are presented and favourable comparisons made with US NRC limits. In response to RO-AP1000-48 (Ref. 50), Westinghouse has recalculated the dose to a member of the public on the site boundary (of a generic site) for the UK and compared the result against the Target 4 offsite BSL for faults with initiating fault frequencies exceeding 1 x 10^{-3} per year. They state that the maximum dose of 0.52 mSv is beneath the 1 mSv BSL.

4.2.8.5 Assessment of SBLOCA Faults

Overview

420 Westinghouse has considered four faults in this category in the EDCD (Ref. 16), as listed at the start of Section 4.2.8.4 above. I have chosen to sample the following three:

- the limiting 10 inch (25.4 cm) cold leg break on the grounds that it is the limiting break size in this category;
- the DVI line break since some of the limiting single failures apply specifically to this fault, and;

- the spurious ADS (or spurious PSV) fault since this is potentially the most frequent fault and so it is important to demonstrate that the fuel does not enter DNB for these faults.

In addition, in its response to RO-AP1000-47 (Ref. 29), Westinghouse has defined a 4 inch (10 cm) cold leg break as its "cliff edge" frequent SBLOCA for which there is a need to demonstrate that there is a diverse means for achieving each safety function.

421 In the sections that follow, my assessment begins with a review of the validation methods applied by Westinghouse to the modelling of SBLOCAs. This is followed by a review of the four faults chosen for sampling. I have also commented on Westinghouse's assessment of radiological consequences from SBLOCAs.

422 Note that the thermal-hydraulic response of the containment vessel to these faults is assumed to be bounded by the double-ended (or 2A) LBLOCA fault which Westinghouse has presented in Chapter 6 of the EDCD. This transient has been assessed during GDA Step 4 but is reported in the containment and severe accident assessment report (Ref. 18).

Methods and Assumptions

423 NOTRUMP has been used to perform the SBLOCA transient analyses presented in the EDCD (Ref. 16). I am aware that the NOTRUMP code has been modified to incorporate modelling of the passive features on AP1000 such as the PRHR heat exchanger, the CMTs, the ADS lines and the IRWST injection lines. For this reason, the validation of NOTRUMP has been reviewed during Step 4 of GDA against the requirements of FA.17 to FA.22 and this is reported in Section 4.4 below as part of the assessment of the passive safety systems for LOCA faults.

424 This assessment identifies the need for a future licensee to analyse the results of commissioning tests that Westinghouse is proposing during the hot functional testing and power ascension on the first AP1000 plant and to confirm that the performance of the ADS Stages-1 to 3 valves and the CMTs are consistent with the claims made in the safety case. These requirements are respectively covered by Assessment Findings **AF-AP1000-FS-36** and **AF-AP1000-FS-37**

425 In addition, I commissioned GRS (Refs 26 and 27) to review the passive safety systems of the AP1000 for potential thermal-hydraulic failure modes. This review is reported in Section 4.5 below. The review is generally supportive of Westinghouse's safety case. However, it questions whether there is a possibility for an interaction between the spargers as they discharge steam into the IRWST following ADS actuation with the potential to challenge the integrity of the IRWST and injection lines. For this reason, I have raised Assessment Finding **AF-AP1000-FS-38**. Given the potential implications for plant layout if this finding is not satisfactorily resolved, I have required that the Assessment Finding should be closed out prior to the pouring of first safety related concrete. Subject to satisfactory resolution of these assessment findings, I judge that the validation evidence for the passive core cooling systems is sufficient to meet the requirements of SAP FA.7.

Limiting Cold-Leg Break (for SBLOCA)

426 The EDCD (Ref. 16) analysis robustly demonstrates compliance with the criteria it sets out to consider. However, like the SGTR analysis, the presented transient analysis is

approximately ten years old and has not been explicitly linked to the GDA Design Reference Point.

427 There is an extended discussion in the EDCD of the core behaviour following a 10 inch (25.4 cm) LOCA fault. However it is known that more recent AFCAP analysis, to date not formally part of the UK submission but probably closer to the GDA Design Reference Point, does not show the core being uncovered and therefore the explanation of the two-phase mixture level is unlikely to be necessary. It is unknown which of the multiple small code and design changes could have caused this difference in prediction. Therefore, at the current time it is difficult to make an assessment against the requirement of FA.17 for the analysis to adequately represent the GDA AP1000 Design Reference Point. Action 1 of GDA Issue **GI-AP1000-FS-02** is therefore directly relevant to SBLOCA.

428 It is likely that the SBLOCA safety case for a 10 inch (25.4 cm) break will probably be simpler and even stronger if the analysis is repeated with the most appropriate AP1000 models. Even in its current status, it is a significant positive feature of the AP1000 safety case that for LOCAs up to 1 ft^2 (929 cm^2) (much larger than that usually considered small in a PWR safety case) the passive Class A1 systems have been shown to prevent the core becoming partially or totally uncovered so preventing clad heat-up.

Confirmatory Analysis

429 In addition to reviewing appropriateness of the NOTRUMP code in its own right, I commissioned AMEC to undertake independent confirmatory analysis of SBLOCA faults using the TRACE code. AMEC used the same US NRC thermal-hydraulic model of the AP1000 as for analysis of SGTR faults.

430 I requested that AMEC investigate the 10 inch (25.4 cm) LOCA fault, with the dual aims of comparing a NOTRUMP prediction with that of the TRACE model, seeing if the core was predicted to become uncovered and needed explanation, and to examine a sample of Westinghouse's records and documentation of LOCA analysis. AMEC used boundary conditions and single failure assumptions consistent with those stated by Westinghouse in the EDCD.

431 AMEC found that Westinghouse's records of its transient analysis, captured in calculation notes in support of the EDCD, were generally clear and self-consistent (compliant with SAP FA.21). However AMEC could not confirm some pressure loss assumptions used in Westinghouse's analysis as these were provided without justification or references. AMEC also noted that Westinghouse's analysis took information from design drawings designated as preliminary. This finding is consistent with my own findings above and will need to be addressed by Westinghouse in its response to Action 1 of **GI-AP1000-FS-02**.

432 AMEC's transient analysis of the 10 inch (25.4 cm) LOCA (Ref. 89) resolves all the phases of the transient up to IRWST injection and the core reflood at approximately 3000 seconds. The key results of this analysis are:

- In the initial stages of the transient, AMEC's predictions are in close agreement with Westinghouse's EDCD analysis.
- Westinghouse consistently predict for all considered SBLOCA faults, that the CMT injection flow rate significantly reduces when the accumulator discharge pressure is reached, and only resumes again once the accumulators are empty. AMEC's TRACE work predicts resumption of CMT injection before the accumulators are empty. Westinghouse has extensive validation evidence and test data to support the behaviour predicted by NOTRUMP so I am not concerned by this disparity.

- In the final part of the transient Westinghouse's NOTRUMP analysis and the AMEC's TRACE analysis are in good agreement on the timing and extent of IRWST injection.
- The TRACE analysis of the 10 inch (25.4 cm) LOCA shows that the core remains covered throughout the transient unlike the NOTRUMP analysis presented in the EDCD (Ref. 16) but consistent with the more recent AFCAP work.

433 Separately from AMEC, GRS has developed an ATHLET thermal-hydraulic model of the AP1000 (Ref. 22). So far this model has mainly been used to look at ATWT faults (see Sections 4.2.3 and 4.2.5). However to benchmark its model ahead of undertaking new analysis, GRS considered a 2 inch (5.1 cm) cold leg SBLOCA fault and compared its ATHLET predictions with the equivalent analysis undertaken by Westinghouse with NOTRUMP (Ref. 23).

434 Like TRACE, ATHLET is a best-estimate code designed to give realistic predictions of plant behaviour. As a result, GRS had to introduce some conservative assumptions to make the ATHLET results comparable with NOTRUMP.

435 GRS concluded that the ATHLET analysis is comparable to Westinghouse's NOTRUMP results. The key results of the GRS analysis are:

- The timings of events during the transient and the liquid break discharge rate calculated by ATHLET are generally in good agreement with NOTRUMP.
- After the initial depressurisation due to the break mass flow, the primary pressure stabilises slightly below secondary pressure. During this period, the CMTs operate in recirculatory mode lasting for several hundred seconds before the CMT pressure balance line starts to void. The CMTs injection rate increases and they drain down causing the primary and secondary pressures to decouple. The plateau in pressure in the first 900 seconds is somewhat lower in ATHLET than NOTRUMP. However the timing of the subsequent actuation of ADS Stage-1 following CMT drain down to 67.5% level is very similar between the codes and from that point the pressure predictions remain similar to the end of the transient.
- In behaviour similar to that found by AMEC with the TRACE code analysis of 10 inch (25.4 cm) cold leg breaks, GRS found that the CMT injection rate did not drop to zero when the accumulators injection commenced. In both TSCs' work, this results in the accumulator injection rate not reaching the same amplitude but lasting longer.
- ATHLET predicts a higher discharge rate from an individual valve during the initial period of ADS Stage-4 operation than NOTRUMP predicts from all four valves. The reason for this behaviour is not clear.
- Following ADS Stage-4 operation, the ATHLET prediction of IRWST injection rate is in good agreement with NOTRUMP predications.

436 Differences between different thermal-hydraulic predictions of complex phenomena are to be expected, especially when comparing predictions from modern best-estimate codes (i.e. ATHLET and TRACE) and an older licensing code like NOTRUMP performed using conservative Appendix K assumptions prescribed by the US NRC. However, both sets of independent analyses are supportive of Westinghouse's NOTRUMP analysis which indicates that the SBLOCA safety margins are respected.

Passive Single Failures (Including Double Ended DVI Line Break)

437 The EDCD analysis has considered active single failures of components associated with the passive safety systems. Failure of one of the four ADS Stage-4 valves to open is

identified as the limiting single failure is modelled in the transient analysis that is presented. However Westinghouse did not consider failures of the check valves in the accumulator and CMT discharge lines, arguing that their failure was "physically unreasonable". As a result of the GDA Step 3 assessment of the AP1000, HSE-ND raised RO-AP1000-47 (Ref. 10) requiring Westinghouse to assess the consequences of these valves failing. If the performance of a safety function is shown to be prevented, then Westinghouse would be required to perform an ALARP assessment to identify if the design could be changed to eliminate the vulnerability to the failure.

438 An innovative feature of the AP1000 is that safety injection is now directly into the reactor pressure vessel using Direct Vessel Injection (DVI) rather than into the reactor coolant loops. This is an advantage in terms of number of redundant safety injection trains that are required because it means that less of the make-up water from the accumulators and safety injection systems is lost if a double-ended break occurs on either the hot or cold leg part of a loop. This is the reason why Sizewell B is provided with four redundant safety injection trains: the double-ended break is assumed to spill the flow from the safety injection train on that affected loop. With preventative maintenance and a single failure each accounting for the unavailability of an injection train there is still one safety injection train available to provide for core cooling in the Sizewell B design. Given that the design intent is that preventative maintenance will not be necessary on the passive systems on the AP1000 design and spillage through a break on a loop is prevented by the use of DVI line injection, the single failure criterion in SAPs FA.6, EDR.2 and EDR.4 can be met with only two trains.

439 Nevertheless, the design of the passive core cooling system does warrant discussion under the single failure criterion requirements defined in SAPs FA.6, EDR.2 and EDR.4 since it is a safety system that consists of the two redundant cooling trains since a break occurring on one of the two DVI lines appears to remove all redundancy with the exception of the CMT discharge valves for which the EDCD claims there will be regular testing and the IRWST injection line check valves, which are provided with redundancy. In particular, there are a number of non-redundant motor operated valves and check valves on the CMT, accumulator and IRWST injection lines.

440 In considering whether the passive core cooling system meets the single failure criterion for the DVI line break fault, it should be remembered that SAP EDR.4 applies only to the safety function and not to a safety system or component. In its response to RO-AP1000-47 (Ref. 32) on passive single failures, Westinghouse argues that the passive core cooling system meets the single failure criterion in this case because the break size is sufficiently small that an individual accumulator or CMT can provide sufficient safety injection flow on their own in the short-term. For longer-term safety injection, the RNS system is claimed to provide a diverse means should failure of the IRWST line occur. The claim on diversity between the accumulator and the CMT using the ADS system is judged to meet the requirements of the SAPs FA.6, EDR.2 and EDR.4 providing the safety analysis is acceptable and adequately validated. The results of the safety analysis are reviewed as part of the following discussion while the validation evidence for the DVI line break is specifically discussed in Section 4.4.3 below.

441 From its passive single-failure analysis performed in response to RO-AP1000-47 (Ref. 20), Westinghouse identified that the following fault sequences need to be reviewed:

- DVI line break with single failure of an ADS-4 squib valve;
- DVI line break with single failure of a CMT check valve;
- DVI line break with single failure of an accumulator check valve;

- DVI line break with single failure of an IRWST injection line normally open MOV, and;
- 2A LBLOCA with single failure of an accumulator check valve.

442 The selection looks sensible. A DVI line break automatically eliminates one of the redundant trains of the passive core cooling system. This makes a failure of one of the ADS Stage-4 valves, of a check valve on either the remaining CMT or the remaining accumulator, or of the isolation valve on the IRWST line of the intact train potentially onerous transients. The 2A LBLOCA with failure of one of the two accumulator check valves will clearly be a limiting fault in terms of accumulator performance. This later fault sequence is discussed further in Section 4.2.8.8 below.

443 However, in addition to these sequences, Westinghouse needs, in my opinion, to consider the following additional failures:

- SBLOCA with single failure of the PRHR isolation valve.

This is because for SBLOCAs corresponding to the smaller range of break size, there is a significant delay in the time for CMT to drain down and actuate the ADS. During this time the decay heat is removed by the single train PRHR. Failure of the isolation valve in the incorrect position will prevent the PRHR from performing this task. These five sequences are reviewed in the following paragraphs.

- *DVI line break with single failure of one ADS Stage-4 valve*

  Failure of one of the four ADS Stage-4 valves during a DVI line break is the standard active failure that Westinghouse already assesses in Section 15.6.5.4B3.5 of the EDCD (Ref. 16). The fault is onerous because only one IRWST line is available for medium-term injection and the CMT on the failed DVI line empties quickly, causing the ADS valve to activate earlier than any other LOCA transient: this maximises the decay heat at the time of actuation. With more limited steam venting due to the single failure in the ADS-4 vent, the RCS pressure remains relatively high making the transition to IRWST injection more onerous than any other SBLOCA. The IRWST injection rate is seen to oscillate as steam flow through the ADS vent path is periodically blocked by liquid coolant filling up the hot leg. Nevertheless, the mixture level in the core presented in Figure 15.6.5.4B-41 demonstrates that the fuel remains covered.

  GRS undertook some independent confirmatory analysis for this fault. The GRS analysis (Ref. 27) strongly suggests that the Westinghouse analysis for the fault reported in the EDCD (Ref. 16) is very conservative because of the bounding nature of the assumption made with regard to the containment back pressure. The GRS analysis suggests that more realistic assumptions about the increase in containment pressure caused by the venting of steam through the ADS Stage-4 valves would demonstrate considerable margin in the Westinghouse analysis of this fault.

  GRS has also performed a statistical uncertainty analysis for this fault by varying key parameters in the ATHLET code model of the AP1000 design in accordance with an assumed probability distribution and statistically sampling to make an estimate of the bounding valve at the 95% confidence level. The results demonstrate that the uncertainty is well defined, relatively small and dominated by the uncertainties in estimating the containment pressure. However, as GRS (Ref. 27) acknowledges, the containment model in ATHLET is fairly crude. To confirm that this view is correct, I have therefore raised Assessment Finding **AF-AP1000-FS-39** for a future licensee to demonstrate that the fault analysis reported in EDCD for the DVI line break fault with

the single failure of an ADS Stage-4 valve provides adequate margin or alternatively to perform coupled code calculations using a validated systems code and a validated containment analysis code to confirm the margins to safety for this fault.

- *DVI line break with single failure of the intact CMT check valve*

  Westinghouse has performed new NOTRUMP analyses (Refs 32 and 98) of the limiting small-break LOCA fault, a Direct Vessel Injection (DVI) line break assuming the single failure of the CMT check valve on the intact DVI line (Ref. 98). The analysis predicts that the core does not uncover during the entire transient and therefore LOCA safety criteria are not threatened.

  A test (Test OSU-APEX-97014, NRC-28) simulating the DVI line break with failure of the intact CMT was performed by the US NRC (Ref. 99) for the licensing of the AP600. Although this confirmed that the core remains covered throughout the transient, it must be recognised that the safety margins for this fault have been reduced in moving from the AP600 design to the AP1000 design. In the UK, the passive single failure of a component in combination with an initiating event is considered to be a credible design basis event. Hence, given the risk significance of this sequence, Assessment Finding **AF-AP1000-FS-40** has been raised for a future licensee to verify that testing exists to address the important phenomena identified in the PIRT for DVI line break fault with the single failure of the CMT check valve on the intact DVI line. Alternatively a scaled integral test (possibly on the APEX facility) may be performed to confirm that the predictions in the safety analysis remain valid. However, given my comments about the validation of NOTRUMP for DVI line faults (see Section 4.4.3), HSE-ND's strong preference is for a test to be performed.

- *DVI line break with single failure of the intact accumulator check valve*

  Westinghouse has performed new NOTRUMP analyses (Refs 32 and 98) of the limiting small break LOCA fault, a Direct Vessel Injection (DVI) line break assuming the single failure of the accumulator check valve on the intact DVI line (Ref. 98). The analysis predicts that the core becomes uncovered to some limited extent. However, the predicted peak clad temperature is limited to 652°C (well below the safety limit adopted by Westinghouse of 1204°C) and the core is re-covered following the start of IRWST injection.

  As with the CMT check valve case, a test (Test OSU-APEX-97015, NRC-29) simulating the DVI line break with failure of the intact accumulator has also been performed by the US NRC (Ref. 100) during the design licensing of the AP600. The core remained covered throughout the transient. Nevertheless, given that the safety margins for this fault will have been reduced in moving from the AP600 design to the AP1000 design and the risk significance of this sequence, Assessment Finding **AF-AP1000-FS-41** has been raised for a future licensee to verify that testing exists to address the important phenomena identified in the PIRT for DVI line break fault with the single failure of the accumulator check valve on the intact DVI line. Alternatively a scaled integral test (possibly on the APEX facility) may be performed to confirm that the predictions in the safety analysis remain valid. However, given my comments about the validation of NOTRUMP for DVI line faults (see Section 4.4.3), HSE-ND's strong preference is for a test to be performed.

- *DVI line break with single failure of the intact IRWST injection line isolation valve*

  Westinghouse has also considered in its response to RO-AP1000-47 (Ref. 32) the consequences of the isolation valve on the intact IRWST injection line being spuriously left in the closed position following a break on the other DVI line. If it occurred, IRWST injection via the intact DVI line would not be possible and the core would eventually be uncovered. This scenario was not considered in the EDCD (Ref. 16). The response to RO-AP1000-47 (Ref. 32) identifies a new safety claim for the UK AP1000, that the Class A2 RNS can be manually aligned and actuated to inject water from the IRWST into the RCS, bypassing the failed valve, and maintaining a two-phase mixture level above the top of the core. This claim adds importance to the functional capability of the RNS to provide diverse means of safety injection on the AP1000 and is discussed further in the section on functional diversity below.

- *SBLOCA with single failure of the PRHR isolation valve*

  In its response to RO-AP1000-47 (Ref. 32), Westinghouse does not consider the potential for a single failure of the normally open PRHR isolation valve following a break within the smaller range of the SBLOCA break spectrum; in this case heat removal from the PRHR is relatively more important as little decay heat will be removed by the break flow. However, Westinghouse has provided a copy of a conference paper (Ref. 132) looking at the 1200 MWe, three-loop Simplified PWR design. This demonstrates that for this design there is adequate time for operator action to actuate the ADS in order to provide adequate cooling to the core. Similar analysis is required for the AP1000. Therefore, as part of its response to GDA Issue **GI-AP1000-FS-05**, I expect Westinghouse to provide analysis of the passive single failure of the PRHR isolation valve in association with a range of SBLOCA breaks.

Functional Diversity for Frequent Faults (4 inch (10 cm) Cold Leg Break)

444 Westinghouse maintain that the frequency of each design-basis SBLOCA fault is low enough such that diversity does not need to be formally demonstrated and is only considered as a “cliff-edge” scenario (and therefore the requirement to claim the Class A2 RNS is not clear-cut). However, both Westinghouse’s own response to RO-AP1000-46 (Ref. 37) and the PSA (Ref. 36) identify the following frequencies:

MBLOCA (between 2 and 9 inch equivalent diameter)[1]	4×10^{-4} per year
CMT cold leg break	9×10^{-5} per year
DVI line break	2×10^{-4} per year
ADS (spurious)	5×10^{-5} per year
SBLOCA (less than 2 inch equivalent diameter)	5×10^{-4} per year
Total	1.2×10^{-3} per year

[1] Including inadvertent PSV opening and a contribution from spurious operation of a single ADS Stage-1 to 3 valve.

445 This list ignores smaller LOCAs such as steam generator tube rupture, PRHR tube rupture and RCS leakage, some of which are very frequent. Furthermore, even with these exclusions, the list sums to greater than 1×10^{-3} per year.

446 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has provided a demonstration that for each safety function there is a diverse means of protection to the Class A1 systems claimed in the EDCD (Ref. 16) following a SBLOCA. Westinghouse argues that a SBLOCA is not a frequent event (i.e. the frequency with which one could occur is $< 1 \times 10^{-3}$ per year). However it has evaluated a 4 inch (10 cm) equivalent diameter cold-leg break as a "cliff-edge" fault to demonstrate the robustness of the AP1000 design.

447 From its diversity analysis response to RO-AP1000-47 (Ref. 20), Westinghouse has identified that the following fault sequences need to be discussed:

- SBLOCA with failure of RCCAs to insert;
- SBLOCA with failure of PMS to trip reactor;
- SBLOCA with failure of CMTs;
- SBLOCA with failure of ADS Stage-4;
- SBLOCA with failure of IRWST injection;
- SBLOCA with failure of containment recirculation;
- SBLOCA with failure of PCS, and;
- SBLOCA with failure of containment isolation.

448 Given the number of sequences to analyse, Westinghouse has defined two bounding sequences for consideration in which a diverse SSC is claimed for each safety function. Westinghouse states that both bounding sequences show compliance with the required safety criteria for SBLOCA and thus the requirements for diversity.

449 Bounding Sequence 1, relies on the following Class A1 passive systems to respond the fault:

- PMS, CMTs, ADS Stage-4 valves, IRWST injection and containment recirculation.

450 No claim is made on the PRHR, accumulators, ADS Stage-1, 2 and 3 valves, CVS or RNS to act.

451 Bounding Sequence 2, relies on a combination of Class A1 and Class A2 SSCs, but none of the Class A1 SSCs claimed in the Bounding Sequence 1:

- DAS, PRHR, accumulators, manual actuation of the ADS 1, 2 and 3 valves, manual alignment of RNS injection and containment recirculation (via RNS lines).

452 Westinghouse has performed transient analysis (Ref. 101) for both bounding sequences using the RELAP-5 code. As noted in the discussion of bleed and feed faults in Section 4.2.3.5 above, no validation evidence has been provided for the application of RELAP-5 to the analysis of the AP1000 design. For this reason, Assessment Finding **AF-AP1000-FS-24**, for a future licensee to provide the validation evidence to support the use of RELAP-5 code or make use of codes validated for the AP1000, is judged to be equally applicable here.

453 These two bounding SBLOCA sequences are assessed in the following paragraphs together with three other SBLOCA sequences: with failure for RCCAs to insert; with failure of the PCS; and with failure of the containment isolation valves:

SBLOCA with Failure of RCCAs to Insert

454 It is noticeable that the bounding sequences do not consider the possibility of SBLOCA with failure of the RCCAs to insert. This sequence is also missing from the ATWT analyses performed in response to RO-AP1000-51 (Ref. 47). In such a sequence the failure of the reactor to trip coupled with the reduction in flow due to the tripping of the RCPs should result in a reduction of reactor power although the margin to DNB could well be challenged. The aim is to ensure adequate cooling of the fuel while maintaining sufficient voiding in the core to avoid a return to criticality. With its strategy of tripping the RCPs and injecting borated water at pressure from the CMTs, the AP1000 is probably well equipped to cope with this fault sequence. However, no transient analysis has been provided to demonstrate that this is the case. This may be because the LOFTRAN computer code that Westinghouse used to assess such ATWT fault sequences is not valid for the saturated RCS conditions that are likely to apply in such circumstances. For this reason, Assessment Finding **AF-AP1000-FS-42** has been raised for a future licensee to perform such an analysis.

SBLOCA with Failure of PRHR, ADS Stages 1-3 and Accumulators

(Bounding Sequence 1)

455 Bounding Sequence 1 (Ref. 101) is the less onerous of the two bounding sequences since the majority of the front line Class A1 safety systems, including automatic actuation of the ADS Stage-4 valves on low CMT level, are assumed to be available. The analysis is performed on a conservative basis with the initial power level assumed to be at 102%. The results show that the core remains covered throughout the transient.

456 The main difference compared with the conventional LOCA sequences examined in the EDCD (Ref. 16) is that the normal depressurisation sequence, with the ADS Stage-1 to 3 valves discharging first before the ADS Stage-4 valves are discharged, is not followed. This means that the ADS Stage 4 valves open at a higher pressure (about 40 bar judged from Fig 5.1-6 of Ref. 101) than normal (typically 7 to 14 bar). This potentially means that the ADS Stage-4 valves will be subject to greater stresses during the initial phase of the depressurisation transient. For this reason, Assessment Finding **AF-AP1000-FS-43** has been raised for a future licensee to confirm the adequacy of the structural integrity of the ADS Stage-4 lines during operation following a SBLOCA fault associated with common mode failure of the ADS Stage 1 to 3 valves and covering a range of break sizes. Given that this assessment finding could potentially affect plant layout this finding will need to be resolved prior to the pouring of first safety related concrete.

SBLOCA with Failure of PMS, CMTs, ADS Stage 4, IRWST and Recirculation injection

(Bounding Sequence 2)

457 Bounding Sequence 2 is a more onerous transient since it requires operator action to perform a manual bleed and feed operation. One of the assumptions made in this sequence is that all the squib valves fail to open. As the use of squib valves on civil PWRs is a novel application of the technology, it is highly desirable to demonstrate a reliably diverse means of protecting against their failure. This is because their use means it is not possible to perform an end-to-end test of the IRWST injection system during the operating life of a plant. This is a shortfall against the requirements of SAP EMT.7, which requires the in-service functional testing of complete systems that are important to safety in so far as is reasonably practicable.

458 The claim on operator action means there is a short period when the core is uncovered after the operator commences bleed and feed at 30 minutes by actuating the ADS Stage-1 to 3 valves until accumulator injection is established. Clad heat-up is predicted, reaching a peak temperature of 677°C, which is comfortably below the 1204°C limit providing operator action is claimed at 30 minutes. No sensitivity studies are performed on the effects of different timings for the operator action. However, the analysis report (Ref. 101) does state that a sensitivity study based upon claiming the low pressuriser level-2 trip on DAS rather than high hot-leg temperature to actuate the PRHR earlier in the transient did avoid a clad temperature excursion. Currently, the DAS (Ref. 16) can trip only the reactor, the turbine, the RCPs and actuate the CMTs on this low level trip signal. For this reason, as part of its response to GDA Issue, **GI-AP1000-FS-05**, I am expecting Westinghouse to review whether it is ALARP to add actuation of the PRHR on this trip parameter as an extra function on DAS. I recognise that there may be disadvantages for cooldown faults in implementing such a modification.

459 Clearly there would be advantages if this claim on operator action could be avoided. The problem is that there is no diverse means of automatically initiating any of the ADS and IRWST injection valves. The sole automatic means of opening these valves relies upon the PMS responding to a low CMT level signal. The diversity provided relies upon operator actuation through the DAS system, which has to be energised to reduce the risk of spurious ADS operation. This is true for both the ADS Stage 1-3 valves as well as the ADS Stage-4 valves. It is clear that the AP1000 designers fully recognise the advantage of diversity between these sets of ADS valves: this is one of the reasons why the ADS Stage 1-3 valves are motor-operated valves while the ADS Stage-4 valves are squib valves.

460 The claim placed on the Class A2 RNS to provide long-term safety injection is new compared to the safety claims presented in the EDCD (Ref. 16). It must be recognised that although the RNS has been upgraded to a Class A2 safety system, it is still essentially a duty system intended to provide the cooling function on a shutdown depressurised reactor during refuelling operations. My understanding is that the RNS is not able to generate a large pressure head. So while it does not require the ADS Stage-4 valves to open in order to inject, it does require the ADS Stage-1, 2 and 3 valves to open. The report presenting the transient analysis for this sequence (Ref. 101) appears to contradict this view, stating that RNS injection is possible even before the ADS valves are actuated. However, a study of a data table in the report (Ref. 101) implies that the maximum pump pressure head of the RNS is 12.8 bar. The RNS also has to be energised and manually realigned by the operator during power operations to perform its safety function. For most of the SBLOCA faults where it is needed to demonstrate diversity, the operator has slightly over 30 minutes in which to perform this realignment. However, in the case of the DVI line break this grace period is reduced to about 15 minutes if actuation of ADS Stage-4 valves is to be avoided (although it is recognised that there is still over 30 minutes available before the intact CMT fully discharges). In this stressful situation, the operator is expected to deduce the location of the break by studying differences in the water levels in the two CMTs in order to determine the optimum RNS alignment for safety injection to avoid a potentially unfavourable interaction with the IRWST system.

461 While recognising that there are Class A1 passive systems capable of delivering the necessary safety functions, it is my judgement that Westinghouse needs to consider further whether there are any possible enhancements to the design of the Class A2 RNS system in its role as a diverse safety injection system. I have therefore raised GDA Issue **GI-AP1000-FS-05** requiring Westinghouse to perform an ALARP assessment to explore the feasibility of enhancing the design of the RNS. The options considered should

include: increasing the pressure head of the system; segregating the water supply of the system from the IRWST; and automating its actuation using a diverse protection system such as the DAS or the Class A2 portions of the PLS.

SBLOCA with Failure of PCS

462 The possibility of SBLOCA with failure of PCS as the ultimate heat sink has already been discussed in Section 4.2.3.5 above. In its response to RO-AP1000-47 (Ref. 32), Westinghouse has argued that the engineering design of the PCS has already taken protection against common mode failure into account such that extra diversity is not required for this function and that the RNS represents a third or "other" means of achieving the function. Nevertheless, Assessment Finding **AF-AP1000-FS-27** has been raised requiring a future licensee to demonstrate that the RNS / CCS / SWS cooling chain systems are adequately sized to provide a diverse heat sink function.

SBLOCA with Failure of Containment Isolation

463 In its response to RO-AP1000-47 (Ref. 29), Westinghouse claims that it has performed analysis of the LOCA fault with failure to isolate containment. It claims that the analysis demonstrates that the PCS is still functionally capable of performing its ultimate heat sink function. None of this analysis has been presented to HSE-ND. Furthermore, no discussion is provided about the functional capability of the containment vessel to prevent radiological releases in these circumstances. It is accepted that Sizewell B is not provided with diverse containment isolation valves, but the AP1000 containment design is very different from Sizewell B. For these reasons, Assessment Finding **AF-AP1000-FS-44** has been raised for a future licensee to demonstrate adequate diverse protection against SBLOCA with failure of containment isolation and to demonstrate that radiological releases are ALARP and meet the requirements of Target 4 of the SAPs.

Spurious ADS or Spurious PSV opening

464 Although the ADS valve fault is classified as a Condition III event in the EDCD (Ref. 16), in its response to RO-AP1000-46 (Ref. 37) it attributed an initiating event frequency of 2.17×10^{-6} per year (5.4×10^{-5} in the PCSR (Ref. 13) and PSA). The PSV fault is a classified as a Condition II event in the EDCD (Ref. 16) but given an initiating frequency of 3.9×10^{-4} per year in the response to RO-AP1000-46 (Ref. 37). It is important to note that the analysis reported in the EDCD (Ref. 16) assumes that PMS remains available to provide protection against the initiating fault despite the fact that it could well have been a malfunction on the PMS that has resulted in the spurious initiation of the ADS. The implications of a more global failure of the PMS resulting in it being unavailable to protect against such a fault are discussed further in Section 4.2.10 below on control and protection faults.

465 The analysis showing that there is a margin to the DNBR safety limit in the initial period after a spurious ADS Stage-1 to 3 valve or pressuriser safety valve opening suffers from the recurring problem of being dated and not clearly linked to the GDA Design Reference Point. The calculation note which supports the EDCD analysis (Ref. 88) often mentions that it is making assumptions based on AP600 analysis. Both the EDCD and Ref. 88 state that the minimum ADS Stage-1 opening time is 25 seconds while predicting that the minimum DNBR occurs at 21.3 seconds. However in response to TQ-AP1000-333 (Ref. 9), Westinghouse has stated that the minimum opening time is 20 seconds.

466 In TQ-AP1000-333, Westinghouse states that the analysis has been repeated with the "latest AP1000 design information" for the AFCAP project and that the limiting DNBR is 1.98, which is well above the DNBR Safety Analysis limit. As discussed above, this AFCAP analysis does not currently form part of safety submission to the UK and it has not been demonstrated that it would be appropriate for the GDA Design Reference Point (see GDA Issue **GI-AP1000-FS-02**).

467 I do not expect any UK-specific analysis to show any safety concerns for this fault. However it is another example that illustrates the need for Westinghouse to provide design-basis analysis either specifically for the GDA Design Reference Point, or to clearly demonstrate why any other presented analysis is appropriate.

468 The EDCD states that the reactor can be tripped following a spurious valve opening on either overtemperature ΔT or pressuriser low pressure reactor trip signal. Transient analysis is presented only for trip on overtemperature ΔT. Based on the fault frequencies, this is sufficient to meet my expectations for the demonstration of diversity in design-basis analysis. However, during site licensing, it will be necessary to show that the set point chosen for pressuriser low pressure protection is ALARP: DNBR protection following a spurious valve opening should be amongst the factors considered. For this reason, I have raised Assessment Finding **AF-AP1000-FS-45** for a future licensee to demonstrate the functional capability of the pressuriser low-pressure reactor trip signal to adequately protect against this fault.

Radiological Consequences

469 Although neither the original EDCD (Ref. 16) analysis of SBLOCA faults nor the additional analysis undertaken in response to RO-AP1000-47 predicts any fuel damage[1], the EDCD presents radiological consequences analysis for SBLOCAs assuming major core degradation and fuel melting. This very conservative approach allows Westinghouse to demonstrate compliance with US NRC dose limits for LOCA faults but it does not allow favourable comparisons to be made against the Target 4 of the SAPs which have a stepped relationship to frequency (Ref. 4). In response to RO-AP1000-48 (Ref. 10), Westinghouse has recalculated the predicted dose to a member of the public on the site boundary assuming 10% of the rods in the core have failed as a result of DNB.

470 To demonstrate compliance with Target 4 of the SAPs, Westinghouse has compared the calculated dose to a member of the public from a SBLOCA (predicted dose of 2.6 mSv for an assumed frequency of 5×10^{-4} per year) with the 10 mSv BSL set for faults with a frequency between 1×10^{-3} and 1×10^{-4} per year. The discussion above on LOCA fault frequencies suggests that it may be more appropriate to make the comparison against the 1 mSv limit for faults with a frequency exceeding 1×10^{-3} per year if it is Westinghouse's intention to bound all LOCA faults up to 1.0 ft^2 with this demonstration.

471 Westinghouse has shown by analysis that DNB and therefore subsequent fuel failures are avoided for the PSV and ADS Stage-1 to 3 opening faults. These faults make a significant contribution to the frequency of "MBLOCA" faults. It may also be possible to show that the smaller breaks considered (less than 2 inch equivalent diameter) do not result in DNB and fuel failures (although Westinghouse has not explicitly done this).

[1] Note that as a Condition III event, Westinghouse assumes a limited amount of fuel damage is possible/permissible and therefore generally do not undertake analysis to show that there is always a margin to DNB and that fuel failures are avoided. The presented transient analysis does show that the fuel melt temperature and oxidation limits are not exceeded.

Assuming 10% fuel damage therefore appears to be very conservative for at least some of the faults contributing to an overall SBLOCA initiating event frequency of 1.2×10^{-3} per year. I am sufficiently satisfied for GDA that future site-specific radiological consequences analysis of SBLOCA should be able to demonstrate compliance with Target 4 of the SAPs. However, in future site-specific radiological consequences calculations care will need to be taken to identify exactly which LOCA faults are being considered and to attribute the appropriate fault frequency (see Assessment Finding **AF-AP1000-FS-46**).

472 I have not specifically assessed any transient analysis of faults involving the failure of small lines carrying primary coolant outside containment. Westinghouse has included the fault within the revised radiological consequences analysis provided in response to RO-AP1000-48 (Ref. 50) which is discussed further in Section 4.6.

4.2.8.6 Findings for SBLOCA

473 Following my assessment of the SBLOCA faults, I am broadly content with the fundamental design of the AP1000 to protect against this class of fault. It is judged that the sizing of the CMTs, accumulators, ADS Stage-1-3 and Stage-4 vent paths, IRWST and containment recirculation injection lines, IRWST and the PCS on the AP1000 are sufficient to provide adequate protection against this class of faults subject to a satisfactory outcome to the additional testing requested below and the commissioning tests proposed by Westinghouse. As with the validation work performed for intact circuit faults, I am impressed with the quality and quantity of the validation test work performed to justify the functional performance of these passive systems.

474 In my opinion, the provision of only two trains of safety injection on the passive core cooling system is adequate and meets the single failure requirements of SAPs FA.6, EDR.2 and EDR.4 based upon the diversity arguments made for the limiting DVI line fault but noting the importance of the Class A2 normal residual heat removal system and its support systems, such as the standby diesel generators, as a risk reduction measure in making the claim on diversity.

475 In particular, it must be recognised that while the sizing of the CMT is sufficient to perform the safety injection role that Westinghouse intended for it, this leaves little time margin for the operator to actuate the RNS following a DVI line fault. I am not yet convinced that the design of the RNS system has been optimised to ensure it can reliably perform its role as a diverse means of long-term safety injection during a SBLOCA fault. From a risk reduction perspective, there are potential advantages in automating its actuation and increasing its pressure head. For this reason, GDA Issue **GI-AP1000-FS-05** has been raised for Westinghouse to perform an ALARP review of the design of the RNS.

476 As noted above, I have raised Assessment Finding **AF-AP1000-FS-38** for a future licensee to confirm that it is not possible for the spargers to interact during ADS discharge potentially threatening the integrity of the IRWST. Given that this assessment finding could potentially affect plant layout this finding will need to be resolved prior to the pouring of first safety related concrete.

477 Given the risk significance of the DVI line break fault sequences, Assessment Findings **AF-AP1000-FS-40** and **AF-AP1000-FS-41** have been raised requiring a future licensee to verify that the testing exists to address the important phenomena in the PIRT or to perform some further testing (possibly at the APEX facility) to confirm the adequacy of the accumulators and CMTs to provide adequate protection against the DVI line break with the single failure of either a CMT check valve or an accumulator check valve associated with the intact DVI line. HSE-ND's strong preference is for additional testing to be performed.

478 I have also raised Assessment Finding **AF-AP1000-FS-43** for a future licensee to confirm the integrity of the ADS Stage-4 lines following a SBLOCA with common mode failure of the ADS Stage-1 to 3 valves to operate. Given that this assessment finding could potentially affect plant layout this finding will need to be resolved prior to the pouring of first safety related concrete.

479 As noted in Section 4.2.3.5 above, further reassurance is required on the sizing of the RNS, CCS and SWS in their role as the diverse "other" means of providing an ultimate heat sink function under Assessment Finding **AF-AP1000-FS-27**. Given that this assessment finding could potentially affect plant layout, I have asked that it be closed out prior to the pouring of nuclear island safety related concrete.

480 The remaining Assessment Findings **AF-AP1000-FS-39**, **AF-AP1000-FS-42**, and **AF-AP1000-FS-44** to **AF-AP1000-FS-46** are items requiring further confirmatory analysis or for Assessment Findings **AF-AP1000-FS-36** and **AF-AP1000-FS-37** support from commissioning tests rather than a fundamental issue with the design and in my judgement they can be closed out as part of the site licensing process.

4.2.8.7 Summary of Westinghouse's Safety Case for LBLOCA

481 The Large-break Loss of Coolant Accident (LBLOCA) resulting from a break in the main piping of the primary circuit hot or cold legs has traditionally been the design basis for the emergency core cooling systems. The worst fault is a guillotine failure of the cold leg pipe adjacent to the reactor vessel nozzle. The effect is a dramatic depressurisation of the coolant in the primary circuit, which converts the coolant to a mixture of steam and water droplets and expels it from the primary circuit. The depressurisation of the vessel upper head is slightly slower than the rest of the circuit and this flow helps to prolong core cooling for a few useful seconds.

482 The job of the engineered safety systems in this fault is to refill the reactor vessel and reflood the core before fuel damage occurs. Release of radionuclides in this event can be limited provided that the fuel remains within the conventional thermal design limits.

483 The safety case for LBLOCA is set out in Chapter 15.6 of the EDCD (Ref. 16) although the analysis has been updated to reflect UK requirements (Ref. 102). The design intent is to provide passive safety injection to refill the vessel in the event of a LBLOCA and to provide passive recirculation of coolant to ensure heat removal and to maintain the fuel in a coolable geometry. While some fuel pin cladding may fail by clad ballooning, the structural integrity of the fuel assembly will be retained.

484 The emergency safety injection is provided from Class A1 passive safety systems acting in sequence: the two nitrogen-pressurised accumulators; the contents of the CMTs; then in the longer term, by gravity from the IRWST; and ultimately the containment sump.

485 In line with UK requirements, the analysis has been extended to consider the case of coincident failure of the check valves on the safety injection pipework connecting one of the accumulators to the plant. This fault sequence has been shown to be tolerable, but has resulted in a tighter constraint on core power distribution than employed previously.

486 The analysis of LBLOCA is carried out using the WCOBRA / TRAC computer code. WCOBRA / TRAC is a thermal-hydraulic computer code that calculates realistic fluid conditions in a PWR during the blowdown and reflood of a postulated LBLOCA. WCOBRA / TRAC is documented in Ref. 103, with its applicability to AP1000 reviewed in Refs 52 and 104. This code has been subject to a rigorous process of qualification in accordance with the requirements of the US NRC as set out in Ref. 105. The code is applied within a framework which allows the variation of a wide variety of parameters,

both within the modelling and the data. This is used to account for uncertainty in physics and in the plant operation.

487 The analysis has been repeated for various values of uncertain parameters until the body of the analysis results encapsulates the likely response with an appropriate level of confidence.

488 The analysis has addressed the consequences of a number of fuel pins failing by ballooning under their own internal pressure and consequentially reducing the space available for coolant flow. The analysis demonstrates that AP1000 fuel is no different from existing fuel in this respect and the body of experimental evidence demonstrating coolability remains applicable (Ref. 106).

4.2.8.8 Assessment for LBLOCA

489 The bounding fault assumed for analysis of LBLOCA is the guillotine failure of the cold leg of the primary circuit adjacent to the reactor pressure vessel. This is referred to as a 2A LBLOCA. It is conventionally assessed as the limiting LOCA fault. I am satisfied that Westinghouse has demonstrated that this is the worst possible fault, short of failure of the vessel itself. This fault is very unlikely and Westinghouse has also examined more frequent faults, but not surprisingly their consequences are more benign and therefore my focus has been on this fault.

490 I have examined the LBLOCA as a design-basis fault because Westinghouse has chosen not to argue that the primary-circuit pipework as a whole is of high integrity, although I note that this argument has been partly made in the US.

491 I have given particular attention to the examination of the issue of fuel damage because the change of the cladding material could potentially affect the applicability of arguments made for earlier fuel designs.

492 Review of the code WCOBRA/TRAC is an important part of the assessment and this has been considered in some detail, but I took benefit from the assessment of an earlier version of this code for Sizewell B analysis and also the assessment done by US NRC. This part of my assessment is reported in Section 4.4 alongside my assessment of other key computer codes.

493 I have given the issue of possible sump clogging by debris some consideration, but I have limited this due to the thorough assessment of the topic made by US NRC (Ref. 107).

494 Consideration of the effect of this fault on the performance of the containment is reported in Ref. 18.

Modelling of Uncertainty

495 The approach to modelling uncertainty is based on the method of Wilkes and does not make any assumptions about the response of the primary circuit model to uncertainty in modelling except that of independence of certain parameters: reasonable measures are taken to address this issue. Details of the approach are found in Ref. 108. This approach for the analysis of LBLOCA was first developed in Germany and is being widely adopted. I judge that the method adopted by Westinghouse has a degree of conservatism that helps reduce reliance on claims of completeness and independence. I therefore judge that the approach meets the requirements of SAP FA.4; a robust demonstration of the fault tolerance of the facility.

Impact of Fault on Vessel Internals

496 The rapid changes in pressure associated with this fault could lead to significant forces on reactor internals: the effect of these forces needs to be determined. Conventionally, the analysis has made very conservative assumptions about the rate at which a breach in the pipework can develop and this has led to modifications to designs. There is a view amongst other international regulators whom HSE-ND has consulted, that these may not have been necessary. However, Westinghouse has not assessed the consequences of the fault on the vessel internals on the basis that the fault has a low frequency. However, since this fault is within the design basis, such an analysis is required. This issue is discussed in greater detail in the Fuel and Core topic area assessment report (Ref. 17), where GDA Issue **GI-AP1000-FD-02** has been raised requiring further analysis. A GDA Issue is appropriate because although it is judged that this work is not likely to lead to substantial modifications to the plant, the work needs to be done early in the design process to confirm that the judgement is correct.

Single Failure Sensitivity Studies

497 The original analysis of the LBLOCA fault for GDA was based on US design requirements. The safety case requirements in the UK differ from the US in that design-basis fault analysis is required to consider all single failures of safety equipment in combination with the fault. This has resulted in a request through TQ-AP1000-673 (Ref. 9) for additional analysis. In the UK, it is required to consider the possibility that when the pressure in the primary circuit drops below the accumulator gas pressure, one of the check valves will stick in the closed position.

498 In the US, the requirements are that only single failures of active systems need to be considered and therefore the emergency core cooling system availability assumptions differ. The difference results in the need to consider a fault sequence with the loss of one out of two available accumulators acting. These accumulators are used to refill the reactor pressure vessel in the event of the original water inventory being lost during depressurisation of the primary circuit. The analysis is reported in Ref. 102. It demonstrates that the combination of the CMTs and the remaining accumulator are sufficient to refill the lower part of the reactor vessel and to reflood the core with only a moderate delay. The fuel temperatures in the US LBLOCA analysis showed a comfortable margin to the fuel embrittlement limit. The UK analysis also does this, but it results in a need to restrict the plant operational envelope and consider uncertainties differently.

499 The most significant change in the UK analysis is the assumption of a more uniform radial power profile. In the UK, this will now be assessed on a best-estimate basis, assuming a uniform distribution of expected radial form factors reflecting the core depletion. This assumption results initially in the requirement to repeat the analysis each cycle, but later this will be needed only if a fuel reload exceeded the values assumed in previous analysis. Assessment Finding **AF-AP1000-FS-47** has been raised for a future licensee to ensure that each fuel reload design remains consistent with the assumptions of made in this calculation.

500 Additionally, the analysis assumes that the core axial power profile does not differ significantly from the target. The US analysis assumed a uniform distribution of axial shapes within the limits provided by the Technical Specification. I accept this relaxation on the basis that sequences with very low expected frequencies need not be included in

the design basis analysis. The LBLOCA fault progression is substantially sensitive to power level: based on Sizewell B experience, I do not expect that the plant will be operated at full power in the presence of a significant xenon transient. Assessment Finding **AF-AP1000-FS-48** has been raised to address this by specifying suitable surveillances to confirm that reactor operation does not differ significantly from these assumptions.

Clad Ballooning

501 In the event of a depressurisation of the primary circuit and loss of the coolant, the internal pressure in the fuel rods causes a hoop stress in the cladding, which tends to lead to clad ballooning. A number of experiments were carried out on Zircaloy-clad fuel in the early 1980s. It became evident that significant blockages of the coolant flow can develop, but these blockages generally have only a small impact on heat transfer from the fuel rods.

502 The change to Zirlo for the cladding potentially results in slightly different fuel deformation and therefore I asked Westinghouse through RO-AP1000-61 (Ref. 10) to provide a comparative assessment of the cladding materials. The analysis is reported in Ref. 106. No significant difference is predicted. The analysis left a degree of uncertainty about the change in material phase that is expected during the fault. There was also uncertainty associated with the translation of fuel pin strain into coolant blockage. To increase my confidence, I commissioned a more detailed analysis using the MATARE code (Ref. 109). This analysis indicated that for the particular conditions considered, the deformation of the fuel pins is unlikely to have a significant adverse effect on fuel safety limits. This satisfied me that coolant blockage is unlikely to be a safety issue in the AP1000 2A LBLOCA fault.

503 In addition to the concern that clad ballooning can lead to coolant blockage, recent Halden experiments have suggested that fuel with very high burnup may behave differently from other fuel if clad ballooning led to failure (Ref. 110). I have considered whether this needs to be addressed in the safety case.

504 The main concern addressed in this CSNI report (Ref. 110) is that fuel relocation and dispersal observed in the Halden LOCA tests may have unexpected consequences. This is linked to fragmentation of the pellet when the fuel concerned had undergone a change in its crystal structure resulting from deposition of fission-product fragments.

505 Ref. 110 reports that such a high-burnup structure has been found when local burnup exceeds 70 MWd/kgU. In the case of the burnups proposed, this region is limited to the outer rim of the pellet. I note that the fuel tested at Halden had suffered transition to a high-burnup structure over an estimated 42% of the pellet volume: this exceeds the expected fraction for the limiting burnups proposed by an order of magnitude. I also note that in recent tests rods in the burnup range proposed have behaved in a similar way to fresh fuel. I therefore conclude that this issue will only need to be addressed if significantly higher fuel burnups are proposed.

Sump Clogging

506 In zones vulnerable to jet impingement, the AP1000 will use reflective metallic insulation that will not be damaged by jet impingement or be transported to the containment recirculation screens. Testing sponsored by the US NRC shows that changing to foil insulation will significantly reduce the likelihood of screen blockage. The amount of

fibrous debris expected to reach the screens is relatively small, although this is dependent on routine housekeeping.

507 I am content that reasonably practical measures have been specified to prevent debris clogging the sump.

4.2.8.9 Findings for LBLOCA

508 As a result of my assessment of the LBLOCA fault, I have raised two Assessment Findings for a future licensee. Assessment Finding **AF-AP1000-FS-47** is to ensure that future fuel reload designs remain consistent with the assumptions made in the LBLOCA analysis for the failure of one of the accumulator check valve sequence. Assessment Finding **AF-AP1000-FS-48** requires a future licensee to propose a suitable surveillance procedure to confirm that the axial power distribution has not deviated from the assumptions of the safety case prior to fuel load.

4.2.9 Support System Faults (Including Loss of Cooling Chain)

4.2.9.1 Summary of Westinghouse's Safety Case

509 Faults in this category result in the loss of essential support systems on the reactor. These faults include loss of Component Cooling Water (CCS) system, loss of the Service Water System (SWS), loss of the CVS, loss of compressed air and the loss of the Heating, Ventilation and Air Conditioning (HVAC) system.

510 Faults in this category are generally considered under the consequences of the fault and are discussed in the other sections of this report. However, on conventional PWRs there is the potential for such failures to produce consequences that do not readily fall into other categories because the failure can result in multiple consequences.

511 In its response to RO-AP1000-46 (Ref. 37), Westinghouse claims that loss of cooling chain systems faults such as loss of the CCS or the SWS are bounded by the complete loss of forced reactor coolant flow fault discussed in Section 4.2.5.3 above and by the loss of spent fuel cooling faults discussed in Section 4.2.11.2 below. Failure of CVS can potentially result in an interfacing LOCA and so it is bounded by the design-basis fault failure of small lines carrying coolant outside containment considered in Section 15.6.2 of the EDCD (Ref. 16). Loss of compressed air is bounded by the loss of normal feedwater fault (together with the loss of the SFW system) discussed above in Section 4.2.3.5. Failures of the HVAC system are identified as resulting only in an increase in air activity levels in affected working areas.

4.2.9.2 Assessment

512 As noted above in Section 4.1.7 above, Westinghouse has acknowledged (Refs 19 and 38) that there is a need to review the PSA list of faults for support systems including loss of the HVAC system and the chilled water systems. Completion of these items has been raised by the PSA lead as Assessment Finding **AF-AP1000-PSA-13** (Ref. 19). Following on from this work there is a need to consider whether any new initiating events identified through this activity need to be included within the design basis list. For this reason, Assessment Finding **AF-AP1000-FS-06** has been raised requesting a future licensee to review the findings of the response to Assessment Finding **AF-AP1000-PSA-13** (Ref. 19) to see whether any of the new initiating events identified need to be considered as potential design basis initiating events.

4.2.9.3 Findings

513 Assessment Finding **AF-AP1000-FS-06** has been raised requesting a future licensee to review the findings of the response to Assessment Finding **AF-AP1000-PSA-13** to determine whether there are any failures in the support systems that need to be considered as additional design basis faults.

4.2.10 Control and Protection System Faults

4.2.10.1 Summary of Westinghouse's Safety Case

514 Faults in this category result in spurious operation of either the control systems or the protection systems on the reactor. In the case of the plant control system (PLS), the control loops potentially affected include power, RCCA position, pressure, pressuriser level, feedwater, steam dump and the rapid power reduction control systems. In the case of the PMS, the faults cover spurious initiation of engineered safety features on the reactor including spurious reactor trip, turbine trip, PRHR initiation, CMT initiation, RCP trip, PCS initiation, ADS Stages 1-3 initiation, ADS Stage-4 initiation, IRWST initiation, containment recirculation initiation, main steamline isolation, main feedwater and start-up feedwater isolation, steam dump isolation, SG blowdown isolation, CVS isolation, and containment isolation. In the case of DAS, the faults cover spurious initiation of engineered safety features on the reactor such as reactor trip, turbine trip, PRHR initiation, CMT initiation, RCP trip, PCS initiation and containment isolation. Other features of the DAS, such as actuation of the ADS Stage-4 squib valves, are not supplied with dc power during normal operation.

515 Faults in this category are generally considered under the consequences of the fault (e.g. failure of the feedwater control system is bounded by the loss of main feedwater fault covered in decrease in heat removal faults in Section 4.2.3.5 above). However, there are some failures that produce consequences that do not readily fall into other categories such as spurious initiation of the pressuriser spray or heater system.

516 In its response to RO-AP1000-46 (Ref. 37), Westinghouse claims that many of these spurious actuations are already considered or bounded by the other design basis faults.

4.2.10.2 Assessment Overview

517 As noted in Section 4.1.7 above, the EDCD (Ref. 16) does not systematically explain how the list of design-basis initiating events considered within fault analysis of Chapter 15 was derived. In particular, no attempt is made to demonstrate that control and protection system faults have been comprehensively considered. The PSA assessment of AP1000 (Ref. 19) has identified under Assessment Finding **AF-AP1000-PSA-13** the need for a future licensee to review the PSA to see if any additional C&I faults need to be included in this list of PSA initiating events. This has been complemented by Assessment Finding **AF-AP1000-FS-06** in the fault studies area requiring a future licensee to review the findings of Assessment Finding **AF-AP1000-PSA-13** to determine whether there are any additional C&I initiating events that need to be included within the list of design basis events to meet the requirements of FA.4 and FA.5.

518 The remainder of this section focuses on reviewing the current safety case with regard to spurious control and protection system faults on the three main control and protection systems (PLS, PMS, DAS).

4.2.10.3 Assessment of Spurious Operation of Plant Control System (PLS) Faults

519 The response to RO-AP1000-46 (Ref. 37) has identified spurious operation of various control loop systems as potential causes of design basis faults considered in the EDCD (Ref. 16). In other cases, the consequences of the spurious operation are considered to be bounded by design basis faults. Below I have listed a selection of design-basis initiating events followed by control loop systems so identified. The list looks plausible, suggesting that Westinghouse has made an attempt to cover the effects of spurious operation of these control loops in a systematic and logical manner but without documenting it within the EDCD (Ref. 16):

- Increase in feedwater flow faults (Feedwater Controller)
- Excessive increase in secondary steam flow faults (Steam Dump Controller)
- Inadvertent opening of SG relief valve faults (Steam Dump Controller)
- Loss of normal feedwater fault (Feedwater Controller)
- RCCA Bank withdrawal faults (Power Controller)
- RCCA Misalignment faults (Rod Controller)
- Spurious CVS actuation (Boron Dilution) (Pressuriser Level Controller)
- Spurious CVS actuation (Increase in RCS inventory) (Pressuriser Level Controller)

520 However, it must be recognised that the PLS is a very complex computer system and so it is not possible to make a judgement as to whether this list is complete and accurate. Furthermore, Westinghouse does not appear to have considered spurious operation of either pressuriser sprays or pressuriser heaters by the pressuriser pressure control system. It is therefore not clear that the requirements of SAPs FA.4 and FA.5 have been met although I recognise that protection is probably provided for these faults by the PMS which can trip the reactor on low or high pressure.

521 In its response to RO-AP1000-46 (Ref. 37), Westinghouse has identified spurious operation of the heaters as a possible initiating event. TQ-AP1000-1099 (Ref. 9) was raised requesting Westinghouse to explain how this event was bounded by a design basis fault in the EDCD (Ref. 16). In its response, Westinghouse argues that spurious operation of a single heater could be counteracted by operation of the pressuriser sprays. If the sprays are not assumed to operate, consistent with design basis assumptions, then Westinghouse argues that the RCS pressure would slowly increase until the high pressure trip set-point on PMS is reached. Westinghouse adds that from a transient analysis perspective, the rate of pressure rise is bounded by the loss of load/turbine trip case. Should reactor trip not occur, then the PSVs would open to protect against the fault noting that there would plenty of time for the operator action to trip the reactor. The explanation seems reasonable but it needs to be captured within the safety case.

522 Although spurious operation of the sprays does not appear to be covered in the EDCD (Ref. 16) or the RO-AP1000-46 response (Ref. 37), Westinghouse has considered it as a frequent event within its response to RO-AP1000-51 (Ref. 47) on ATWT analysis, classifying it, slightly unusually, as a decrease in reactor coolant inventory fault. Westinghouse has explicitly modelled the ATWT event corresponding to failure of the PMS to trip and the results are shown in Fig 7.6-1 to 7.6-4. This transient initially lowers the primary circuit pressure until the core outlet fluid becomes saturated at about 375 seconds. The reduction in pressure will challenge the margin to DNB although no assessment of DNB is presented within the report. For this reason, Assessment Finding

AF-AP1000-FS-49 has been raised for a future licensee to confirm that the fuel does not enter DNB during this transient.

523 In the case of the ATWT with the rods failing to insert, Westinghouse states that the PMS will trip the turbine causing a heat-up transient that compensates for the initial fall in pressure and effectively transforms the transient into a turbine trip ATWT event, as discussed in Section 4.2.3.5 above. I accept the arguments of Westinghouse.

524 In summary, initiating events due to failures of the PLS system have not been systematically reviewed and documented by Westinghouse in the PCSR. For this reason, Assessment Finding **AF-AP1000-FS-50** has been raised for a future licensee to demonstrate that any spurious failures associated with the PLS are either bounded by other design basis initiating events or provide explicit design basis analysis as part of the safety case.

4.2.10.4 Assessment of Spurious Operation of Plant Monitoring System (PMS) Faults

525 As with the PLS, the EDCD (Ref. 16) makes no attempt to systematically demonstrate how potential spurious actuation signals from the PMS to engineered safeguard features have been considered within the list of design basis faults in Chapter 15 of the EDCD. However, it is clear that the following have been identified:

- Turbine Trip (including Reactor Trip and Spurious MSIV closure fault);
- loss of normal feedwater (Main Feedwater Isolation);
- spurious PRHR actuation;
- spurious CMT actuation, and;
- spurious ADS actuation (of a single ADS Stage-1, 2 or 3 valve).

526 However, from a study of the above transients, it is clear that Westinghouse makes the assumption that these events are all protected by the PMS. This fails to consider that it was a malfunction on PMS that was responsible for the spurious initiating event, and so the PMS may not be available to protect against the fault it initiated. For this reason, RO-AP1000-82 (Ref. 10) was raised requesting Westinghouse to demonstrate that these spurious actuations were already covered by the existing design basis analysis, or to provide a revised safety case. Westinghouse was effectively being asked to demonstrate that for such faults there is a suitably qualified diverse means of protection independent of the PMS.

527 In its response to RO-AP1000-82 (Ref. 111), Westinghouse has performed a brief review of each of the engineered safety feature actuation signals on the PMS with additional clarification obtained through TQ-AP1000-1173 (Ref. 9). In most cases Westinghouse argues that the event is either benign or that it is already covered by an ATWT transient due to failure of the PMS to trip. For example, normal feedwater isolation is covered by loss of normal feedwater with failure of PMS to trip. In most of these sequences DAS is expected to trip the reactor and the turbine and to initiate the PRHR, CMTs and PCS. Westinghouse also notes that the PLS would first try to reduce turbine power and initiate the SFW system, although it should be recognised that the PMS can isolate this system as well. While I accept that DAS should be able to protect against this fault, I note that the PSVs will lift and there will be a conditional failure probability of about 1×10^{-2} per demand that the PSVs will fail to reseat. With the PMS assumed to be unavailable, the operator would need to initiate ADS Stage-4 valves to provide protection against the consequential LOCA (partial ADS with injection from the RNS represents an alternate

option). Depending upon the assumed initiating frequency for the spurious initiation, this event could be a risk-significant sequence in the PSA.

528 The AP1000 is unique amongst PWR designs in that the PMS may spuriously actuate equipment such as the ADS Squib valves, which can automatically depressurise the reactor. Westinghouse has identified potential problems with the current design approach in that spurious actuation of the ADS Stage-4 valves may challenge the structural integrity of the ADS Stage-4 lines. There are also difficulties with ensuring a rapid reactor trip following actuation of the ADS Stage-1 to 3 valves due to the limited trip parameters currently available on the DAS: the pressuriser low-level trip would not be a reliable and effective indicator of such faults due to the discharge of coolant though the pressuriser to the ADS 1-3 lines. For this reason, Westinghouse is proposing a hard-wired blocker device to inhibit PMS from spuriously actuating the ADS valves. The design intent is to ensure that the reliability of the ADS system is not compromised by the blocker device, while ensuring that spurious actuation is avoided or is a beyond design basis event below 1×10^{-7} per year. The progress with the safety case and the design of the ADS blocker device will be monitored under Action 1 of Control and Instrumentation topic area GDA Issue **GI-AP1000-CI-04** (Ref. 134).

529 HSE-ND also has concerns about the adequacy of the safety case covering spurious operation of the containment recirculation valve. In its response to TQ-AP1000-1289 (Ref. 9), Westinghouse concedes that without operator action to isolate the spuriously opened containment recirculation valves, the water in the IRWST will drain into the containment sump resulting in the consequential unavailability of the PRHR and IRWST injection capability. The reactor may trip, either as a result of the flooding of the containment sump causing consequential tripping of essential support systems located in these areas such as the RCPs, or by operator action as required by the internal flooding hazard safety case (see Section 4.2.13). Then post-trip cooling would be solely reliant upon operation of the SFW system (assuming the SFW is also not isolated by the PMS initiating event). Westinghouse is considering its position on this matter and may consider applying the blocker device to the containment recirculation valve as well. For this reason, Action 2 of Control and Instrumentation topic area GDA Issue **GI-AP1000-CI-04** (Ref. 134) has been raised to monitor progress with the development of this safety case.

530 There may also be advantages in Westinghouse applying the proposed blocker device to the IRWST injection line squib valves. In the event of these spuriously opening, protection is currently provided by non return valves. However, depending on the initiating event frequency assigned to the spurious operation of these valves, it may be necessary to consider the single failure of one of these valves. If a reliable design of blocker device is developed, it would not be too difficult to extend its application to these valves as well.

531 In my view, given the brevity of the response to RO-AP1000-82 (Ref. 111), there is still a need for a systematic and comprehensive design-basis safety case covering the spurious operation of the other engineered safeguard features on the PMS to be included within the PCSR. For this reason, Assessment Finding **AF-AP1000-FS-51** has been raised for a future licensee to provide such a case.

4.2.10.5 Assessment of Spurious Operation of Diverse Actuation System (DAS) Faults

532 Initiating events due to failures of the DAS system have also not been systematically reviewed and documented by Westinghouse in the EDCD (Ref. 16). However, given that all the engineered safeguard features provided on the DAS form a subset of those provided on the PMS, and given that the PMS would be available to provide protection following a spurious signal from the DAS, it is my judgement that it should be possible to

make a satisfactory safety case for the DAS. Nevertheless, this needs to be confirmed by a future licensee. For this reason, Assessment Finding **AF-AP1000-FS-52** has been raised for a future licensee to demonstrate that any failures associated with the DAS are either bounded by the existing design basis initiating events or provide explicit design basis analysis for such faults as part of the safety case.

4.2.10.6 Findings

533 In my opinion, the fault sequence analysis covering control and protection faults on the AP1000 design is the least mature area of the safety case. However, I recognise that Westinghouse has been proactive in identifying the ADS blocking device as a potential design modification to provide increased protection against the spurious actuation of the ADS valves. This design proposal could benefit other faults such as the spurious initiation of the containment sump recirculation valves or the other squib valves. To monitor progress with the safety case and the design of the blocker device, Actions 1 and 2 of Control and Instrumentation topic area GDA Issue **GI-AP1000-CI-04** have been raised. Action 1 covers spurious operation of the ADS valves and Action 2 covers spurious operation of the containment recirculation valves.

534 In addition, a number of assessment findings have been raised covering general aspects of the control and protection fault safety case. Assessment Finding **AF-AP1000-FS-06** requires a future licensee to review the conclusions of the response to Assessment Finding **AF-AP1000-PSA-13** to see if any additional spurious initiating events need to be considered within the design basis. Assessment Finding **AF-AP1000-FS-49** requires a future licensee to confirm that fuel will not enter DNB in the ATWT event following the spurious operation of the pressuriser sprays with common mode failure of the PMS. Finally, Assessment Findings **AF-AP1000-FS-50**, **AF-AP1000-FS-51** and **AF-AP1000-FS-52** require a future licensee to provide a safety case covering initiating events caused by spurious PLS, PMS and DAS actuation signals within the PCSR.

4.2.11 Spent Fuel Pool Faults

4.2.11.1 Summary of Westinghouse's Safety Case

535 The design basis safety case discussed here is that provided for loss of cooling and loss of water inventory faults, resulting in a threat to the cooling of the spent fuel. I have not assessed the criticality safety case for the spent fuel pool or any civil engineering concerns. These aspects of the spent fuel pool safety case are assessed in Refs 114 and 115.

536 Westinghouse's safety case for the spent fuel pool has changed significantly during GDA Step 4 from that presented in the EDCD and assessed for GDA Step 3. This has principally been in response to RO-AP1000-54 (Ref. 10). The design basis safety case assessed for GDA Step 4 is that presented in Ref. 112.

537 The spent fuel pool is cooled in normal operation by the Class A2 Spent Fuel Pool Cooling System (SFS). In addition, the Class A2 RNS has the capability of being aligned to take over the cooling function of the SFS. This mode of cooling is available when the RNS is not needed for normal shutdown cooling of the reactor (and potentially long-term safety injection for the reactor).

538 Both the RNS and SFS are comprised of two redundant, separated trains of equipment that are powered by redundant and separated power supplies. The RNS and SFS heat exchangers are cooled by the Class A2 CCS which in turn is cooled by the SWS. The

CCS and SWS also comprise two redundant and separable trains that are powered by redundant and separated power supplies.

539 Westinghouse state that the AP1000 Spent Fuel Pool design is based on a defence-in-depth approach that relies on both Class A2 active systems and Class A1 passive systems to provide protection against potential heat-up leading to damage to the stored fuel.

540 The Class A2 cooling chains are designed not only to reliably support normal operation, but also to minimise the demand on the passive systems. In case of a total failure of the active cooling (i.e. due to problems with the SFS/RNS, CCS, SWS, their supporting systems, or AC power supplies), the principal means of ensuring cooling of the spent fuel is provided by the Class A1 inventory of water in the pool and additional Class A1 make-up sources that can provide passive makeup to the spent fuel pool.

541 Following a postulated complete loss of the Class A2 cooling chain, the pool will heat up and boil off water, providing the necessary cooling to the spent fuel. Water above the fuel, even at reduced water levels, provides sufficient shielding since no operations immediately above or in the pool fuel handling area would be conducted. The spent fuel pool water inventory is thus the principal means (Class 1) of fulfilling the Category A safety function of cooling and shielding the fuel in the spent fuel pool.

542 There are a number of piping connections to the spent fuel pool which, in the event of a break, could result in both a reduction in water inventory and a loss of cooling. A break in the Class 2 pipework of the SFS is a scenario that Westinghouse considered in the EDCD. Ref. 112 additionally considers the breaks in the Class 1 RNS suction line, in the Class 1 Fuel Transfer Canal drain line, in the Class 1 Cask Loading Pit piping connection to the RNS, and in the spent fuel pool piping connection to the refuelling pit common water supply/drain header[1].

543 Westinghouse has identified three significant safety claims to protect spent fuel from loss of cooling and loss of water inventory faults:

- Safety Claim #1 - The AP1000 design provides enough water inventory from Class A1 sources to ensure that the fuel will remain covered for at least 72 hours following all design basis events, even assuming unavailability of all non-Class 1 systems.
- Safety Claim #2 - The AP1000 design provides a robust Class A2 active cooling chain and Class 3 and non-classified operational systems that minimise the demands on the Class A1 passive systems. The design is such that the probability of onset of boiling is 4.42×10^{-4} per year.
- Safety Claim #3 - In addition to the Class A1 sources designed to ensure the fuel remains covered for at least 72 hours (Safety Claim #1) and in addition to the Class A2 cooling chain designed to minimise the demands on the Class A1 Systems (Safety Claim #2), there are additional, diverse Class 2, 3, and non-classified sources that (1) provide diverse protection in the case of failures in both the Class A2 cooling chains and the Class A1 passive systems, and (2) also ensure long-term fuel coverage for loss of cooling events.

544 Ref. 112 summarises calculations predicting the times to boiling and subsequent exposure of fuel for various spent fuel inventories and refuelling scenarios. This

[1] The Class 1 designation of the pipework reflects a requirement to maintain its integrity, rather than any protective safety function such as cooling.

establishes the time, if at all, makeup water needs to be provided to ensure that the fuel remains covered. Ref. 112 also sets out what operator actions (principally which valves need to open and close) need to be taken to establish makeup water flow to the spent fuel pool.

545 With respect to Safety Claim #2, it is noted that for RNS breaks, make-up from Class A1 sources is supplied via a Class 2 line. This is because the Class A1 route to the spent fuel pool from the Class A1 PCCWST source is through the RNS. If the route of the water inventory loss from the spent fuel pool is the RNS, an alternative route must be provided. Westinghouse considers a Class 2 line to be acceptable due to the frequency of the event and the significant time available (over 1 day) before any makeup is in fact necessary. Additionally, for the vast majority of the fuel cycle, no spent fuel pool make-up is required to reach the 72 hours before the stored fuel is uncovered.

546 Westinghouse has proposed two design modifications to support the submitted safety case:

- The calculated frequency for the loss of Class A2 active cooling of the spent fuel pool is dominated by the probability of losing the CCS and the SWS. To reduce the frequency of the total loss of active cooling of the spent fuel pool so that pool boiling becomes an infrequent event (< 1 x 10^{-3} per year), Westinghouse has initiated a design change proposal to enhance an existing connection of the Fire Protection System (FPS) to the CCS such that fire protection water can be provided by an engineered route at a flow rate sufficient to cool the RNS and SFS heat exchangers.
- To relieve the pressure build up within the fuel building as a result of the steam produced by pool boiling, the original AP1000 design had blow-out panels which opened to atmosphere on elevated ambient temperature. Westinghouse has predicted that the radiological consequences to a member of the public from steam released via this unfiltered route are small (< 1 mSv). However these calculations do not take into account uncertainties due to possible fuel crud becoming mobile due to the boiling. Also, a non-filtered route to atmosphere is not consistent with SAPs ECV.1, ECV.2 and FA.7. As a result, Westinghouse has initiated a design change proposal to add a passive filtering capability to the blowout panel flowpath.

547 These design changes were identified late in GDA Step 4 and therefore neither of them has been formally supplied to HSE-ND for assessment. It should also be noted that the modifications to the Class 2 systems for the AP1000 50Hz standard are also important in reducing the frequency of boiling.

4.2.11.2 Assessment

548 During Step 4 Westinghouse has substantially revised the safety case for loss of cooling and loss of water inventory events in the spent fuel pool. It is proposed to incorporate a number of changes to the design originally presented in Ref. 16, and greater visibility has been provided on the claims made on SSCs and operators to protect and mitigate against identified faults.

549 A significant improvement on Westinghouse's original position is that total loss of active cooling to the pool is now predicted to be an infrequent event. Sizewell B has a similar safety case with make-up water being provided following a total loss of cooling, so there is a precedent for this approach. It is recognised that the AP1000 is not only capable of providing make-up water to keep the fuel covered and adequately cooled in a boiling pool from Class A1 sources for 72 hours, but it also has additional diverse (active) sources available.

550 The revised safety case provided by Ref. 112 was submitted to HSE-ND only at the end of GDA Step 4 and so there has not been time to assess any of the evidence to support these claims.

551 Completion of the proposed design changes is fundamental to making an acceptable safety case which limits the frequency of pool boiling to less than 1×10^{-3} per year and which meets HSE's expectations on ventilation and preservation of barriers set out in SAPs ECV.1, ECV.2 and FA.7. Details of these modifications need to be supplied to HSE-ND for assessment within GDA.

552 While I have briefly reviewed the new safety case for the spent fuel pool, colleagues in other technical discipline areas have not been able to review the design and safety case with sight of the new claims placed on SSCs and operators. I also have not seen how Westinghouse has or intends to incorporate the new claims within the PCSR and supporting documents.

553 It is therefore not possible to finalise the assessment of the spent fuel pool within GDA Step 4. I have raised a GDA Issue **GI-AP1000-FS-01** requiring Westinghouse to provide the further substantiation and finalised design proposals to enable further assessment across different technical discipline areas. Action 1 requires Westinghouse to review the claims made in the new spent fuel pool design basis safety case and ensure that they are cascaded throughout future revisions of the PCSR. Action 2 requires Westinghouse to provide further details on the identified design changes to HSE-ND.

554 In the Fault Studies area, Ref. 112 does not address to my satisfaction the consequences of faults occurring while fuel is being moved above the racks. It is also not clear whether it is planned for the RNS to be available without restriction for spent fuel pool cooling in response to operational requirements, or if its use will be subject to time constraints defined by Technical Specification. This has relevance for the GDA Issue on the RNS design for RCS safety injection following a LOCA. No safety claims were made on the function of the RNS in the EDCD other than for its piping to retain its integrity. However, as a result of Step 4 ROs, claims are now made in the UK safety case for both the reactor and the spent fuel pool. Further information is therefore required from Westinghouse to identify if these claims conflict.

555 Both of these issues need to be addressed in the response to Action 3 of **GI-AP1000-FS-01**, and the latter point on the RNS needs to be considered in the response to **GI-AP1000-FS-05**.

556 The assessment of Westinghouse's safety case for spent fuel pool criticality is beyond the scope of this report. However it has been an area of on-going development during GDA Step 4 through the vehicle of RO-AP1000-73 (Ref. 10). A final strategy for ensuring criticality safety was not fixed during Step 4 and as a result **GI-AP1000-RP-01** has been raised (see the Step 4 Radiological topic area assessment report, Ref. 114). Once the criticality GDA Issue has been satisfactorily addressed and a strategy agreed, the PCSR safety case for spent fuel pool faults needs to clearly state how criticality control is maintained for the loss of cooling and pipe break faults considered, with consideration given to the deliberate addition of unborated makeup water.

557 Technical Specifications themselves are outside the scope of GDA but it is noted that neither Westinghouse's existing AP1000 Technical Specifications presented in Ref. 16 nor the availability controls on Class A2 systems presented in Ref. 113 will reflect the new claims made on SSCs for the Spent Fuel Pool.

4.2.11.3 Findings

558 As a result of the assessment of the response to RO-AP1000-52 (Ref. 112) covering the provision of a design basis safety case for the spent fuel pool, GDA Issue **GI-AP1000-FS-01** has been raised.

559 Action 1 requires Westinghouse to review the new claims identified in the response to RO-AP1000-52 and ensure they are disseminated throughout the AP1000 safety case, bringing them to the attention to HSE-ND assessors in other technical disciplines.

560 Action 2 requires Westinghouse to provide further details on the two identified design changes.

561 Action 3 requires Westinghouse to address remaining Fault Studies concerns about stranded fuel and the potentially conflicting claims on the availability of the RNS.

4.2.12 Shutdown Faults

4.2.12.1 Summary of Westinghouse's Safety Case

562 With the exception of CVS malfunction leading to a decrease in boron concentration, shutdown reactor faults are not considered in Chapter 15 of the EDCD. Following a review of shutdown risk (Ref. 116), US NRC requested that Westinghouse perform a systematic assessment of the shutdown risk issue to address areas identified in the review, as applicable to the AP600 design. The AP1000 design is based extensively on the AP600, and the SSCs that were important in maintaining a low shutdown risk for AP600 are generally the same design and / or have the same design-basis with respect to reducing shutdown risk for the AP1000. Therefore Westinghouse concluded that the assessment of the shutdown risk for the AP600 was applicable to the AP1000. A summary of the assessment of the shutdown risk issue for AP1000 is given in Appendix 19E of the EDCD. Despite Chapter 19 of the EDCD being nominally about PSA, Appendix 19E includes design basis evaluations of events that can occur during shutdown.

563 Like other PWRs, the AP1000 has a number of operational modes (six). The definition of Mode 4 has been specifically rewritten for the AP1000 with an upper temperature limit of 420°F (216°C) that corresponds to the RCS temperature that can be achieved by the passive safety systems 36 hours after shutdown.

564 Appendix 19E describes a number of AP1000 design features incorporated for shutdown operations, including:

- RCS hot-legs and cold-legs vertically offset to permit draining of the steam generators for nozzle dam insertion with the hot-leg level much higher than traditional designs.
- RCS instrumentation designed to accommodate shutdown operation.
- A step nozzle connection between the RNS and the RCS hot-leg. This has the twin effects of lowering the RCS level at which a vortex in the RNS pump suction line occurs and restricting the air entrainment into pump suction line should a vortex occur.
- ADS first, second and third stage valves are open whenever the CMTs are blocked during shutdown operations with the reactor vessel upper internals in place. This provides a vent path to preclude pressurisation of the RCS if decay heat removal is lost. It also allows the IRWST to automatically provide injection flow if actuated on loss of decay heat removal. In addition, two of the four ADS Stage-4 valves are

required to be available during reduced inventory operations to preclude surge line flooding following a loss of the RNS.

- The steam generators are equipped with permanently mounted nozzle dam brackets, which are designed to support nozzle dams during refuelling operations. The dams can be installed via the steam generator manway with the hot-leg water level at the nominal water level for mid-loop operations.
- The secondary side of the steam generators can be cooled during shutdown by recirculating their contents through the blowdown system heat exchanger. This ensures that the SGs can be cooled and so reduces the chances of reverse heat flow into the primary circuit so protecting the RCS from the challenges of a low temperature overpressure event when it is water solid.
- The passive residual heat removal system provides decay heat removal during power operation and is required to be available in shutdown Modes 3, 4, and 5, until the RCS is open. In these modes, the PRHR heat exchanger provides a passive decay heat removal path.

565 In shutdown modes, safety systems are required to be taken out of service to prevent them actuating spuriously as the pressures and temperatures drop (e.g. accumulators and some safeguard signals). Other systems are opportunistically allowed to be taken out of service for maintenance (in a controlled manner) as the capability required to perform individual safety functions reduces. Therefore, although in most cases the consequences of faults from at-power will be limiting, demonstrations of adequacy for at-power faults will not always be sufficient for shutdown faults as fewer or different SSCs are claimed to provide protection during the transient.

566 Each of the design basis accidents and transients considered in Chapter 15 of the EDCD is reviewed in Appendix 19E with respect to low power and shutdown modes. Claims and arguments are presented to conclude that for the majority of faults, full power operation is bounding. The only fault for which additional analysis was judged necessary was a double-ended rupture of one of the two cold-legs in the RCS loop without the PRHR heat exchanger, just after the accumulator isolation.

567 The double-ended cold-leg guillotine break has been analysed using the WCOBRA/TRAC computer code. The analysis calculates a peak clad temperature of 771°C, which is less than the US NRC limit of 1204°C.

568 During shutdown, once pressures and temperatures have reached a low level (Mode 4, defined in the Technical Specifications), cooling of the RCS is switched from the SGs to the RNS. The failure of the RNS (having been successfully put into operation) is a design-basis fault. However it is a fault unique to shutdown operations and is not considered in Chapter 15 of the EDCD. Appendix 19E does consider this type of failure; identifying two faults with loss of normal residual heat removal system (one in Mode 4 with the RCS intact and one in Mode 5 with the RCS open) for analysis.

569 To facilitate RCS maintenance, the AP1000 design allows the reactor coolant level to be reduced to the hot-leg (mid-loop) level; the RCS pressure boundary may then be opened. Westinghouse anticipates that the most limiting shutdown condition is mid-loop and therefore assumes this reduced level in its analysis of RNS faults. Note that although this is an appropriate and conservative assumption for the design-basis analysis, it is for a future operator to decide whether to undertake maintenance at mid-loop with the fuel in-situ in the pressure vessel or to remove all the fuel to the spent fuel pool. Mid-loop maintenance activities with fuel in the pressure vessel are out of scope of GDA and

Westinghouse has not provided a safety case or an ALARP argument for such operations.

570 For the loss of normal residual heat removal fault in Mode 4, it is assumed that the RNS has been placed in operation 4 hours after reactor shutdown. It is assumed that off-site power is lost, resulting in the loss of the RNS cooling and thus complete loss of heat removal from the RCS. As the pressure and temperature increases in the RCS, mass inventory is lost through the RNS relief valve. If no reliance is placed on operator action and only automatic actions are claimed, a CMT actuation signal is generated on pressuriser low level and the PRHR heat exchanger isolation valve opens. As the CMT level decreases, the first stage ADS set-point is reached, resulting in a rapid depressurisation of the RCS. When the CMT level reaches the fourth-stage ADS set-point, two of the four fourth-stage paths open (assuming one path is out of service due to maintenance and another fails as a single active failure). This final ADS stage allows IRWST injection to begin.

571 If earlier operator actions are credited, then the CMT and PRHR isolation valves would open but ADS actuation can be avoided.

572 The results of transient analysis for both automatic and manual safety actuation following the loss of normal residual heat removal fault in Mode 4 are presented in Appendix 19E of the EDCD. The core stack mixture level is shown to be maintained above the top of the core active fuel height throughout the transients. At the end of the transients, the reactor coolant mass inventory is stated to be acceptable and increasing.

573 For the loss of normal residual heat removal fault in Mode 5, it is assumed that the RNS is in operation 24 hours after reactor shutdown with the ADS Stage-1, 2 and 3 valves open and the RCS vented to the IRWST. The SG secondary side is assumed to be drained and therefore unable to provide a secondary heat sink. The CMTs and PRHR are assumed to be out of service as permitted by the Technical Specifications. Only two of the four fourth stage ADS paths are assumed to be available; one of the two IRWST injection paths is assumed to be out of service in accordance with the Technical Specifications.

574 The transient analysis for this fault has assumed loss of off-site power, resulting in loss of RNS flow. The subsequent increase in reactor coolant temperature leads to voiding in the core and in the hot-leg, with inventory being lost through the open ADS stages. RCS hot-leg level instrumentation prompts manual and / or automatic actuation of the fourth-stage ADS valves and initiation of IRWST injection. A time delay is provided on the automatic actuation to allow time for the operators to restore decay heat removal using operational or non-Class 1 safety systems prior to actuating the PXS. The time delay with an alarm in the containment serves to protect maintenance personnel. One of the two available ADS Stage-4 valves is assumed to fail to open as a single active failure.

575 The core stack mixture level is shown to be maintained above the top of the core active fuel height throughout the transients. At the end of the transient, the core stack inventory is restored to above the middle of the hot-leg elevation and the down-comer mixture level is above the DVI nozzle elevation. The EDCD therefore concludes that, assuming the operator acts before or at the point at which the hot-legs empty (at which point an automatic signal would be generated), one ADS Stage-4 valve is effective in reducing the system pressure so that the consequences of the fault are acceptable.

576 In addition to the systematic consideration of shutdown modes on Chapter 15 faults, US NRC specifically requested additional analysis to show that the passive systems can bring the plant to a stable safe condition and maintain this condition so that no transients will result in the specified acceptable fuel design limit and the pressure boundary design

limit being violated. Also no high energy piping failure with unacceptable consequences should result. Westinghouse has responded to this requirement by presenting transient analysis of a loss of ac power event from power. Using just the passive systems, the core average temperature is shown to reach the required 420°F in approximately 34 hours. This mode of operation can last up to 72 hours. However if no ac power is available 22 hours after the event, the EDCD states that the ADS will be actuated automatically (the operator can veto this action). Operation of the ADS in conjunction with the CMTs, accumulators and IRWST reduces the RCS pressure and temperature below the 420°F upper limit for safe shutdown.

4.2.12.2 Assessment Overview

577 The passive philosophy of the AP1000 is not inconsistent with the provision of a robust safety case for shutdown faults. With the primary pressures already reduced, there are fewer immediate challenges in reaching pressures low enough for large quantities of water to be provided to the core under natural forces. In addition, the AP1000 design includes a number of features for shutdown operations, building upon lessons learned from operating PWRs. These design features are welcomed as they show that Westinghouse has taken steps to ensure that risks from shutdown faults are reduced. However, it is noted that some of these features are defence-in-depth provisions or operational systems which are not formally claimed in the design-basis safety case.

578 Westinghouse's calculation of the risk from shutdown faults and the appropriateness of AP600 analysis is assessed and discussed in Ref. 19.

579 In my GDA Step 3 assessment report (Ref. 6), I commented that the EDCD provided logical arguments as to why no additional transient analysis was needed for shutdown faults beyond that presented for at-power faults. However, this fell short of my expectations for a design basis safety case as set out in SAPs FA.4 to FA.9. This led to RO-AP1000-54 (Ref. 10) being raised for Westinghouse to address during GDA Step 4. My assessment of the design basis safety case presented in the RO response is presented below.

4.2.12.3 Assessment of Design Basis Shutdown Safety Case

580 The response to RO-AP1000-54 (Ref. 112) does the following:

- Identifies faults that can occur at shutdown, including faults that have at-power equivalents, faults specific to shutdown, and faults specific to refuelling.
- Summarises the availability / unavailability of Class A1 passive core cooling equipment during shutdown modes.
- Summarises the AP1000 design features provided for shutdown safety, reflecting what is presented in the EDCD.
- Summarises the rationales presented in the EDCD for why most shutdown faults are bounded by the analysis of equivalent at-power faults.
- Presents transient analysis for a double-ended cold-leg guillotine break in Mode 3 with the accumulators isolated, reflecting what is presented in the EDCD.
- Presents design-basis safety cases for loss of RNS faults, including transient analysis.

- Identifies and discusses breaks in RNS piping both inside and outside the containment during RNS operation.

581 Ref. 112 does not present a safety case for faults specific to the refuelling mode (Mode 6) other than identifying them.

582 Ref. 112 does clearly set out what passive Class A1 systems are available for core cooling during shutdown modes. It also provides a list of all shutdown faults identified by Westinghouse as being within the design basis, in accordance with SAP FA.5. However there is no significant new information on which SSCs are claimed for individual shutdown faults (which can be different from at-power faults) or why it is demonstrably permissible to remove SSCs from service in accordance with the Technical Specifications (for example, if single failure criteria are still met with SSCs out of service). It is my understanding that a future Fault Schedule will provide further information, but this was not available to accompany the RO-AP1000-54 response. Appendix 19E of the EDCD and Ref. 112 do not provide initiating event frequencies for the identified faults and do not discuss the requirements for diverse means of fault protection if the frequency is $> 1 \times 10^{-3}$ per year. Therefore the AP1000 documentation provided to date for shutdown faults still fails to meet my expectations for such a design basis safety case.

583 A clear example of this shortfall is the discussion provided in the EDCD and Ref. 112 for increase in reactor coolant inventory faults (i.e. a malfunction of the CVS) occurring with the RNS in operation. During at-power operations and shutdown modes without the RNS, malfunctions in the CVS are protected against by the inclusion of automatic CVS isolation functions in the PMS (high pressuriser level). When the RNS is in operation, this signal and isolation are not available. Instead, low-temperature over-pressure protection of the RCS pressure boundary is provided by the RNS relief valves. The design-basis fault sequence for this shutdown fault is therefore significantly different to the at-power equivalent fault.

584 Appendix 19E of the EDCD and Ref. 112 do not mention either the frequency of faults which place demands on the low-temperature over-pressure protection or the safety classification of the claimed SSCs (although Ref. 33 does classify the RNS suction relief valves as Class 1). The RNS is a two-train system, each train with its own suction relief valve. The Technical Specifications presented in Chapter 16 of the EDCD state that one relief valve is required to be operable in Mode 4 when any cold-leg temperature is ≤ 275°F (135°C), in Mode 5, and in Mode 6, when the reactor vessel head is on. There is no discussion of whether this arrangement is single-failure proof. The sizing of the valves is stated to be sufficient to meet the US NRC's 10 CFR 50 Appendix G steady-state temperature limit. This limit is possibly entirely appropriate but there is no justification given for why this US Federal Regulation is applicable for the UK and no evidence is referenced to show how this limit is met.

585 The design basis shutdown safety case presentation in Ref. 112 for loss of RNS faults is superior to that provided for other faults. The claims on Class A1 systems are identified, single failures are discussed, and transient analysis is presented to support the claims made. However, Westinghouse has acknowledged that the transient analysis reported for these RNS faults has not been fully documented (TQ-AP1000-972, Ref. 9) and therefore no references or calculation notes were available for detailed assessment. Westinghouse has initiated a corrective action process to investigate and remedy this deficiency. It is suspected that the undocumented transient analysis for shutdown faults is at least 10 years old and was not repeated as part of the AFCAP work. It is therefore inevitable that old computer models were used and that the design assumptions were not necessarily appropriate for the proposed UK design. Action 1 of **GI-AP1000-FS-02** is therefore equally applicable to shutdown faults and given that the original analysis is not recorded,

the way to address the deficiency in available documentation is expected to be new analysis appropriate for GDA Design Reference Point provided as part of the GDA Issue response.

586 Breaks in the RNS piping outside of the containment during Modes 4, 5 and 6 were not considered in the EDCD. Westinghouse states that this is in accordance with US NRC guidelines which specify that pipe ruptures need to be considered only in systems that operate with high-energy conditions for more than 2% of the system operating time or 1% of plant operating time (including shutdowns). The RNS does not have high-energy conditions for sufficient time for these US criteria to be met and therefore pipe breaks in the system were not considered.

587 This generic rule-based approach would not be acceptable in the UK: significant further justification would be needed to support such an approach for a specific application. However, Westinghouse pre-empted such a conclusion in their response to RO-AP1000-54, by choosing not to provide evidence and actions (e.g. a commitment to undertake inspections) to support the appropriateness of these criteria for the UK: instead RNS pipe breaks are to be considered within the design basis. Descriptions of the various fault sequences are provided (the sequence and claims are different depending on the shutdown mode and whether the break is inside or outside containment). No transient analysis is provided in Ref. 112 for these faults nor a link to any pre-existing transient analyses which can be assumed to bound them. The expected responses of Class A1 SSCs to the faults are described but there are no details on break sizes, assumed reduced availability of safety systems (in accordance with the Technical Specifications) and single failure assumptions.

588 For a RNS break outside of containment in Modes 4 and 5, Westinghouse has identified that there would be no automatic containment or RNS isolation signal. This is because the containment pressure would not rise since the break is located outside of the containment: the low PZR level signal does not generate an S-signal. As a result, inventory from the RCS, CMTs and IRWST would be lost outside of containment until manual action was taken. With no operator action within 30 minutes, a significant amount of inventory could be lost to the break, potentially enough to impede the establishment of long-term core cooling. In Ref. 112, Westinghouse has identified this as an open item that they intend to resolve in the following way, either:

- show that sufficient inventory can be retained assuming that the operator will act at 30 minutes, justifying the current design, or;
- show that the addition of a containment isolation signal based on ADS actuation would provide adequate core cooling and be ALARP.

589 Westinghouse needs to close out this open item and the other underdeveloped aspects of the safety case for this newly considered fault as part of the broader efforts to resolve GDA Issue **GI-AP1000-FS-07**. In addition, I am concerned that there could be other potential pipe breaks not covered by a robust “Incredibility of Failure” safety case justification, but excluded from the design basis. However, **GI-AP1000-IH-03** Action 1 has been identified in the Internal Hazards topic area assessment report (Ref. 117) for Westinghouse to perform quantitative assessment of the consequences of postulated pipe failures. Successful resolution of this GDA Issue is anticipated to address my concerns about potential gaps in the consequence analysis presented in AP1000 safety case.

4.2.12.4 Radiological Consequences

590 Ref. 112 does not present any discussion of the radiological consequences of shutdown design-basis faults while Appendix 19E of the EDCD only considers the following shutdown risks relevant to the radiological consequences methodology:

- gas waste management system leak or failure;
- liquid waste management system leak or failure (atmospheric release);
- release of radioactivity to the environment via liquid pathways;
- fuel handling accident, and;
- spent fuel cask drop accident.

591 The EDCD states that, even amongst this short list, the first three are not considered because US NRC's "Standard Review Plan" does not require these faults to be assessed. This is not on an acceptable justification for not considering these faults further in the UK.

592 In the response to RO-AP1000-48 (Ref. 50), Westinghouse has stated (without any supporting justification or analysis) that there is no release of activity to the environment for loss of RNS faults in shutdown Modes 4 and 5. Given that such a fault causes a steam release from the primary circuit while containment hatches and air locks are open, this apparently significant claim needs considerably more justification including links to grace times for containment closure following such an event. Westinghouse has provided no comment on the dose to workers from shutdown faults or any assumptions on additional measures (e.g. evacuation within a period of time).

593 In principle, all design basis faults, including shutdown faults should be compared with Target 4 of the SAPs. In practice, as with the thermal-hydraulic transient analysis, it may be possible to assume that the shutdown faults are bounded by the consequences calculated for equivalent at-power faults although in my opinion, it is not clear that this could be demonstrated for worker exposure. However, if this is the approach adopted, this should be clearly stated: the initiating fault frequencies determining the BSL targets would need to reflect the contribution from shutdown faults. Other faults, e.g. loss of RNS faults should be addressed separately on their merits. It follows that it is not currently possible to say that the AP1000 design basis safety case for shutdown faults meets the requirements of FA.7.

4.2.12.5 Limits and Conditions

594 The derivation of Technical Specifications is outside the scope of GDA. The EDCD and Ref. 112 do refer to the reduced availabilities allowed by the generic Technical Specifications presented in Chapter 16 of the EDCD in their discussion of specific faults. In a small number of cases, transient analysis is presented which supports the availability requirements specified in Technical Specifications. However it would be difficult to systematically define a set of limits and conditions attributable to the design-basis safety case from the EDCD and Ref. 112. Although it is principally a requirement on a future site licensee, it is not very clear how the currently available design-basis analysis for shutdown faults will provide an input to Technical Specifications, safety limits, and safety classification etc as required by SAP FA.9.

595 The Cross-cutting topic area assessment GDA Issue, **GI-AP1000-CC-01**, requires Westinghouse to set out the necessary arrangements to advise a future licensee on the limits and conditions necessary to ensure safety (see Ref. 144). This includes the requirement to ensure that there is an appropriate link between the analysis documented

in the safety case and the associated operational limits and conditions. Shutdown faults need to be considered as part of this response.

596 In the absence of an assessed Fault Schedule, it is not currently possible to say that the AP1000 design-basis safety case for shutdown faults meets the requirements of ESS.11 and FA.8. GDA Issue **GI-AP1000-FS-07** requires additional evidence (expected to be in the form of transient analysis) to support the availability assumptions/requirements set out in the Technical Specifications adopted by a future site licensee. The Technical Specifications or the assumptions in the design basis safety case may need to be modified if the evidence does not demonstrate that the assumptions are ALARP.

4.2.12.6 Findings

597 Westinghouse has not presented an acceptable design-basis safety case for shutdown faults in the EDCD and Ref. 112. Therefore GDA Issue **GI-AP1000-FS-07** has been raised. The most appropriate way to address this shortfall is through a future update of the PCSR (Ref. 13). The following are required as part of the response:

- Shutdown faults need to fully integrated into Chapter 9 of the PCSR (Ref. 13). If the available at-power design basis analyses (i.e. the thermal-hydraulic analysis, radiological consequences and claims on SSCs) are assumed to bound or apply to shutdown faults, then this needs to be clearly stated in the PCSR, justified as necessary, and initiating fault frequencies updated accordingly. Fault sequences which are significantly different in terms of consequences or claims on SSCs from their at-power equivalents need to be considered separately, but with the full rigour expected for design basis analysis (i.e. SAPs FA.4 to FA.9). This includes consideration of limiting single failures, demonstration of diversity for frequent faults and discussion of the consequences including those to workers.
- Technical Specifications are outside the scope of GDA. However it is expected that the worst normally permitted configuration of equipment should be clearly stated (in the PCSR) for faults in each applicable shutdown mode in accordance with SAP FA.6.
- Faults during refuelling modes need to be covered by the PCSR.
- The safety case for RNS pipe breaks outside of containment needs to completed, with arguments, transient analysis, design change proposals etc. presented and cited in the PCSR as necessary.

598 A Fault Schedule is needed to reflect and support the safety case for shutdown faults. This is also to be reported via a future update of the PCSR, as part of the requirements of an additional GDA Issue **GI-AP1000-FS-08**.

599 The transient analysis presented in the EDCD for loss of RNS cooling faults needs to be repeated. This should be done using the latest computer models and making design assumptions appropriate for the GDA Design Reference Point as part of the response to Action 1 of GDA Issue, **GI-AP1000-FS-02**. The new analysis needs to be presented and cited in the PCSR as necessary.

600 In the response to the GDA Issue on Limits and Conditions raised in the Cross-cutting topic area assessment report (Ref. 144), **GI-AP1000-CC-01**, Westinghouse needs to set out how availability assumptions made in the design-basis safety case for shutdown faults will be reflected in new site-specific Technical Specifications. GDA Issue **GI-AP1000-FS-07** has been raised for additional evidence to be provided to support the availability assumptions/requirements for the shutdown safety case set out in the Technical Specifications adopted by a future site licensee.

4.2.13 Internal Hazards

601 Faults in this category are caused by on-site hazards that have the potentially to result in the loss of essential support systems on the reactor. These faults include fire, internal flooding, steam releases from pressure systems, dropped loads, missiles and hydrogen explosions. From the perspective of transient analysis, faults in this category are generally bounded under the consequences of one of the faults presented in the previous sections.

602 The GDA Step 4 assessment of internal hazards is reported in the internal hazards assessment report (Ref. 117) and so internal hazards are not discussed in any detail in this report. Nevertheless, the area has been briefly reviewed from a Fault Studies perspective as it provides an indication of how the interface between internal hazards and Fault Studies has been handled by Westinghouse. Internal fire and internal flooding have been sampled to gain an understanding of the approach. However it should be emphasised that the assessment of the adequacy of the detailed substantiation covering the functional capability of fire barriers and flooding compartments to protect against such hazards is provided by the internal hazards assessment report. In particular, it is noted that the Internal Hazards topic area assessment report (Ref. 117) has raised six GDA Issues, **GI-AP1000-IH-01** to **GI-AP1000-IH-06**, covering internal fire, flooding, pressure-part failure, explosion, missile, and dropped loads respectively, which require Westinghouse to improve the presentation of the internal hazards safety case for the AP1000.

603 Westinghouse's basic approach to the treatment of internal hazards is to ensure that the consequences of internal hazards are controlled and limited so that the safety functions performed by SSCs required to bring the plant to the safe shutdown state are not affected by the hazard. In addition, design provisions are made to limit the failure of SSCs so as to prevent other consequential internal hazards.

604 In the case of internal fires, the original safety case was presented in Appendix 9A of Chapter 9 of the EDCD (Ref. 16) with supplementary information on the systems required for safe shutdown provided in Chapter 7.4 of the EDCD. During GDA Step 4, Westinghouse has revisited the internal fire safety case in the internal hazard topic report (Ref. 118). The basis of the safety case is to ensure that the reactor is tripped and remains as an intact circuit with heat removal achieved using the PRHR cooled by the IRWST with the ultimate heat sink provided by the PCS. Long-term reactivity control is provided by the supply of borated water from the CMTs. Since the discussion focuses on achieving safe shutdown, no detailed justification is given as to how the plant achieves the initial controlled state with the reactor tripped and the safety systems actuated. As noted earlier in Section 4.2.4, the PRHR, CMTs and PCS do not require electrical ac or dc power for their operation and will automatically be actuated should there be a loss of the Class A1 dc power supply. However, there is no discussion provided on how these systems will be actuated if the Class A1 dc power supplies remain available despite the presence of a fire. However, Appendix 9A appears to claim the operator to trip the reactor: this seems to contradict the claim that AP1000 does not require operator action for a period 72 hours following any design-basis event.

605 To provide protection against fires, the AP1000 plant is divided into a number of fire areas and fire zones. Fire areas are three-dimensional spaces designed to contain a fire that may exist within them. The boundaries of fire areas are separated by fire barriers. Fire zones are three- dimensional spaces within a fire area. They are defined as the entire zone of influence in which a fire will be contained. All equipment in any one fire zone is assumed to be rendered inoperable by the fire while systems outside a fire zone

are considered free of fire damage. The containment represents a single fire area, while the remaining buildings outside the containment are divided into a number of fire areas. The containment is a single fire area because of the need to maintain the free exchange of gases in the containment following other design-basis events. However, it is divided into a number of fire zones to prevent fire spread by separation of equipment by distance.

606 The safe shutdown systems discussed above are located mainly within the containment building. To provide confidence that these systems are protected, the safety case systematically reviews each fire area outside containment, on an area by area basis, and each fire zone within containment, on a zone by zone basis, to identify the sources of combustible material and the principal systems located within that area or zone. This information is used to establish whether the safe shutdown function can be achieved. Generally, this is achieved by claiming that a redundant train located in a different fire area or fire zone is able to achieve the safety function. For example, fire zone AF 11206 is inside containment and contains the valves on one train of the PXS including accumulator A, while fire zone AF 11207, which is also inside containment, contains the valves on the other train of the PXS including accumulator B.

607 In the original assessment reported in Appendix 9A of the EDCD (Ref. 16) the assessment methodology assumed that a concurrent single active component failure (independent of the fire) could not occur. In the revised assessment reported in internal hazard topic report (Ref. 118) this assumption has been revised and it is now claimed that an unrelated single failure cannot prevent the safety function from being achieved although this is not explicitly demonstrated within the area by area or zone by zone assessments; it is not obvious that passive single failures have been considered. Westinghouse will need to expand this discussion further in their response to GDA Issue **GI-AP1000-IH-01** to meet the requirements of SAPs FA.6, EDR.2 and EDR.4.

608 The safety case claims that no fire in any fire zone can cause spurious actions which could cause a breach in the reactor coolant boundary, defeat the Class A1 decay heat removal capability, or increase the reactivity of a shutdown reactor. Importantly, the safety case states that automatic depressurisation is not required to achieve the safe shutdown state following a fire and that spurious actuation of the ADS is avoided.

609 In the case of the ADS Stage-4 squib valves, the safety case claims that spurious actuation of the squib valves is prevented by the design of the squib valve controller circuit: multiple hot shorts would be required for actuation; potential hot short locations are physically separated; and there are provisions to remove power from the fire zone by operator action local to plant outside the affected fire area. The safety case claims that no postulated fire can spread to the hot short locations before the operator can remove power supplies.

610 In the case of the ADS 1, 2, and 3 MOVs, the safety case claims that each vent path has two MOVs in series such that spurious operation is prevented by the use of physical separation of control circuits for the two series valves. Additionally, there are provisions to remove power from the fire zone by operator action local to plant outside the affected fire area. Again, the safety case claims that no postulated fire can spread to the hot short locations before the operator can remove power from the fire zone.

611 From a transient analysis perspective, the safe shutdown systems listed above are those expected to operate following a loss of normal feedwater fault with coincidental loss of the start-up feedwater system. The transient is discussed in Section 4.2.3 above. A feature of this transient is that because of the limited heat removal capacity of the PRHR, it is likely that a PSV will lift and reseat during the transient. In its response to TQ-AP1000-289 (Ref. 9), Westinghouse acknowledges that there is a conditional probability of 1×10^{-2} per

demand (Ref. 9) that a PSV could fail to reseat following any demand to lift. This suggests that a fault sequence with a fire in coincidence with a SBLOCA cannot be discounted. Therefore maintaining an intact circuit following a fire cannot be completely assured, even if the spurious operation of ADS valves is avoided.

612 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has briefly considered the provision of diversity to cope with the possibility of a frequent fire. The response provides only an outline justification since there is no discussion of how the location of the fire affects the safety systems that would be claimed. So the arguments will need to be expanded further as part of the response to the Internal Hazards topic area GDA Issue **GI-AP1000-IH-01** (Ref. 117) which requires Westinghouse to provide a design basis safety case for internal fire hazards. Nevertheless, it is clear from the response to RO-AP1000-47 (Ref. 29) that manual bleed-and-feed using the ADS and IRWST injection is being claimed as the main diverse means of achieving decay heat removal and borated water injection; the SFW system and the CVS are noted as "other" possible diverse means. This claim on bleed-and-feed appears to potentially contradict the strategy of getting an operator to isolate the power supplies to the ADS valves in an affected fire zone since the operator could potentially disable the bleed-and-feed capability. It should also be recognised that it may be difficult for an operator to deduce within which fire area or fire zone a fire is located. Given that the ADS actuation is based upon a 2-out-of-4 voting logic, it is also unclear why it is necessary for the operator to isolate the power supplies to the ADS circuits in an affected fire zone. In its response to GDA Issues **GI-AP1000-IH-01** and **GI-AP1000-CI-04** covering spurious ADS operation, Westinghouse will need to clearly explain and justify this strategy.

613 The safety case notes that spurious operation of the valves at the interface between the RNS and the RCS is avoided by locking out the power supplies to the valves during normal power operations. While this eliminates the possibility of spurious operation of the valves during a fire, it will clearly reduce the reliability of the RNS to act as a diverse means of safety injection during a SBLOCA and will need to be reviewed as part of GDA Issue **GI-AP1000-FS-05**.

614 As noted above, operator action is claimed to trip the reactor (and presumably to actuate the safety systems). No discussion is provided to justify the adequacy of this protection or to substantiate how it will be achieved on an area-by-area or zone-by-zone basis. This issue will need to be substantiated in the response to GDA Issue **GI-AP1000-IH-01**.

615 In the case of internal flooding, the original safety case is presented in Chapter 3.4 of the EDCD (Ref. 16) with supplementary information on the systems required for safe shutdown provided in Chapter 7.4 of the EDCD. During GDA Step 4, Westinghouse has revisited the internal flood safety case in the internal hazard topic report (Ref. 118). The basis of the safety case depends upon the source of the flooding. If the source of the flooding is not associated with a LOCA event, then the approach is to ensure that the reactor is tripped and remains as an intact circuit with heat removal achieved using the PRHR cooled by the IRWST with the ultimate heat sink provided by the PCS. Long-term reactivity control is provided by the supply of borated water from the CMTs. As noted earlier for the internal fire hazard, these systems do not require electrical ac power for their operation and will automatically be actuated should the Class A1 dc power supply be lost. The operator is claimed to trip the reactor based upon level indications in those areas where there is a source for potential flooding. In the case of flooding in containment, this would be based upon level alarms from either the containment sump level monitoring system or the flood-up level instrumentation. If the source of flooding is a LOCA event the reactor will be tripped automatically. Safe shutdown is ensured using the CMTs and accumulators, with injection initially from the IRWST and ultimately from

recirculation flow from the containment sump. This results in the containment being flooded up to a level above the RCS piping. With the exception of the LOCA event, where reactor trip is automatic, the need for operator action to trip the reactor appears to contradict the claim that for any design-basis event there is no need for operator action for 72 hours.

616 The safe shutdown systems discussed above are predominately located within the containment building. To provide confidence that these systems are protected, the safety case systematically reviews each compartment room by room and floor by floor to identify the possible sources of flooding, essential equipment located within that compartment, and the associated flow rates and flood levels. It is then established whether the safe shutdown function can be achieved, generally by claiming that a redundant train located in a different compartment is able to achieve the safety function.

617 For example, compartment PXS-A (Room 11206) is located inside containment and contains the components on one train of the passive core cooling system while compartment PXS-B (Room 11207), which is also inside containment, contains the components of the other train of the passive core cooling system. The PXS-A and the PXS-B compartments are physically separated and isolated from each other by a structural wall so that flooding of one compartment cannot flood the other: a curb is provided at the top of the compartments where they penetrate through the maintenance floor. These compartments drain into the main reactor vessel cavity compartment (Room 11105). Reverse flow through these floor drains is blocked by redundant Class A1 backflow preventers in the drain lines. If the flooding rate exceeds the ability of the floor drain lines to drain the water from one of these compartments, or if the floor drain is blocked, the water level in that compartment increases to the entrance curb elevation. If the flooding continues, the water overflows the curb and immediately drains to the RCS compartment. In this way, flooding of more than one of the two passive core cooling system compartments is avoided even if the flood level reaches the maximum flood level for a LOCA based upon the combined inventory of the RCS, the two accumulators, the two CMTs and the IRWST flooding the containment.

618 From a transient analysis perspective, the flooding safety case for an intact circuit is very similar to the fire safety case discussed above in that the safe shutdown systems that are claimed are those expected to operate following a loss of normal feedwater fault with coincidental loss of the start-up feedwater system, as discussed in Section 4.2.3 above. The transient analysis for LOCA events is explicitly considered within Section 4.2.9 above.

619 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has briefly considered the provision of diversity to cope with the possibility of a frequent internal flood. The response provides only an outline justification since there is no discussion of how the location of the flooding affects the safety systems that would be claimed: these arguments will need to be expanded further in the response to GDA Issue **GI-AP1000-IH-02**. Nevertheless, it is clear from the response to RO-AP1000-47 (Ref. 29) that manual bleed and feed using the ADS and IRWST injection is claimed as the main diverse means of achieving decay heat removal and borated water injection although the start-up feedwater system and the CVS are noted as other possible means.

620 A final general comment is to note that internal hazards are not presented within the list of design basis initiating events provided in Westinghouse's response to RO-AP1000-46 (Ref. 37) and so it is difficult to see whether the barriers protecting against the fault are appropriately categorised and classified. For this reason, as part of its response to GDA Issue **GI-AP1000-FS-08**, Westinghouse is expected to include internal hazards on the fault schedule (or some other equivalent format to be agreed with the regulator).

4.2.14 External Hazards

621 Faults in this category are caused by off-site hazards that have the potential to result in the loss of essential support systems on the reactor. They include natural hazards such as seismic events and external flooding. From the perspective of transient analysis, faults in this category are generally bounded under the consequences of the faults presented in previous sections.

622 The assessment of external hazards is reported separately since it has its own technical topic area (Ref. 115). External hazards are therefore not discussed in any detail in this report. Nevertheless, the area has been briefly reviewed from a fault study perspective as it provides an indication of how the interface between external hazards and Fault Studies has been handled by Westinghouse. The seismic hazard has been selected as an area for sampling to gain an understanding of the approach adopted. It is emphasised that assessment of the detailed substantiation covering the functional capability of the design to withstand a seismic event is provided by the external hazards assessment report (Ref. 115).

623 Westinghouse's approach to external hazards is to ensure that the consequences of external hazards are controlled and limited to ensure that the safety functions performed by SSCs required to bring the plant to the safe shutdown state are not affected by the hazard. In addition, design provisions are made to limit the consequential failure of SSCs to prevent consequential internal hazards.

624 In the case of the seismic hazard, this is generally achieved by seismic qualification of those Class A1 SSCs required to withstand the loads from the design basis seismic event without loss of function. In addition, those SSCs, whose continued function is not required, but whose structural failure or interaction could degrade the functioning of Class A1 SSCs, are seismically qualified to withstand the loads from the design-basis seismic event without loss of structural integrity.

625 In its response to RO-AP1000-47 (Ref. 29), Westinghouse has briefly considered the provision of diversity to cope with the possibility of a frequent design-basis seismic event. As with the safety case for internal hazards, the basis of the case is to ensure that the reactor is tripped and remains as an intact circuit with heat removal achieved using the PRHR cooled by the IRWST with the ultimate heat sink provided by the PCS. Long-term reactivity control is provided by the supply of borated water from the CMTs. Diversity is provided by claiming manual bleed and feed using the ADS and IRWST injection as the means of achieving decay heat removal and borated water injection. However, in contrast with the internal hazards safety case, no claim is placed upon active Class A2 systems for the frequent seismic event apart from the DAS and the dc electrical supply system as the Class A2 safety systems are not generally seismically qualified to continue to function following the infrequent design basis seismic event. As a result, Westinghouse do not claim any provision of diversity for the ultimate heat-sink function should the IRWST or PCS, which are seismically qualified to Class A1 standards, suffer a common mode failure.

626 It is note that external hazards are not presented within the list of design basis initiating events provided in Westinghouse's response to RO-AP1000-46 (Ref. 37) and so it is difficult to see whether the barriers protecting against the fault are appropriately categorised and classified. For this reason, as part of its response to GDA Issue **GI-AP1000-FS-08**, Westinghouse is expected to include external hazards on the fault schedule (or some other equivalent format to be agreed with the regulator).

4.3 Assessment of Validation Evidence for Passive Safety Systems for Non-LOCA Faults

627 It should be recognised that claims on natural circulation cooling in PWRs are not novel and that the height of the PRHR above the core is comparable with that of the SGs. Nevertheless, it is essential that there is high confidence in the functional capability of the PRHR given its claimed reliability of 2×10^{-4} per demand in the PSA. For this reason, I have chosen to review the LOFTRAN validation for modelling of the PRHR for the following important phenomena:

- the flow resistances through the PRHR loop for natural circulation conditions, and;
- the primary and secondary side heat transfer correlations used for the PRHR.

628 The validation evidence of the LOFTRAN code for application to non-LOCA faults on the AP1000 is summarised in the AP1000 code applicability report (Ref. 52). Heavy use is made of test results and validation evidence developed for the AP600 reactor design. There are two steps to the validation argument for the AP1000. The first step of the argument uses the AP1000 PIRT and scaling assessment report (Ref. 53) to argue that the operating conditions and the PIRT assessment developed for non-LOCA events on AP600 remains applicable for the AP1000: this argument is based upon the similarities of the two designs after taking into account the increased component capacities on the AP1000 to accommodate and compensate for the higher core power rating. The AP1000 code applicability report (Ref. 52) therefore argues that the validation tests reported in the AP600 LOFTRAN code applicability report (Ref. 49) used to justify the validation of LOFTRAN for AP600 are equally applicable for use on the AP1000.

629 The second step of the argument uses the supporting references to the AP600 LOFTRAN code applicability report to justify the validation for AP600. The main references are the AP600 verification and validation final report (Ref. 42) which presents a series of full pressure and full height integral test performed at the SPES-1 and SPES-2 test facilities (Refs 54 and 55) and the separate effect AP600 PRHR heat exchanger tests (Ref. 58).

4.3.1 Component Sizing

630 With regard to the performance of the PRHR, the AP1000 PIRT and scaling report (Ref. 53) notes that:

- the reactor thermal power has increased by 73% in going from AP600 to AP1000.
- the diameter of the PRHR inlet and outlet pipework has been increased from 25 cm to 38 cm such that the overall flow resistance through the PRHR has been reduced by a factor 3 in going from the AP600 to the AP1000: this is sufficient to increase the natural circulation flow rate through the PRHR by 74%.
- the PRHR heat transfer area has been increased by 22% by increasing the number of PRHR tubes and their length;
- the PRHR elevation is unchanged but the thermal centre of the core has been lowered on the AP1000 by 30 cm slightly increasing the buoyancy driving head;
- the SG MSSV set-points have increased from 75 bar to 82 bar resulting in an increase in the hot leg temperature entering the PRHR inlet from 291°C to 297°C, and;
- the mass of water in the SGs at the SG narrow range trip set-point has been increased by a factor 2.39 (or 139%).

631 Westinghouse argues that the increase in flow rate to match the increase in reactor power will ensure the buoyancy head driving the natural circulation flow is essentially unchanged. Increasing the flow rate will also increase the heat transfer such that the heat removal capacity of the PRHR has been increased by an amount comparable to the increase in core power. In addition, the SG secondary side inventory has increased by significantly more than the increase in core power and so more than compensates for any slight delay in the time until the PRHR matches the decay heat level in the core. Since the surface area of the PRHR has only increased by 22%, the average heat flux through the PRHR tubes will increase by 42% to account for the increase in reactor power level. Westinghouse argues that this increase in the heat flux is still within the range of the measurements performed on the PRHR heat exchanger test for AP600 since measurements were also made for the much higher flow conditions corresponding to forced flow with the RCPs in operation. In particular, Westinghouse notes that the conditions are still well within the critical heat flux margins on the secondary side. On the basis of these observations, Westinghouse argues that the heat transfer correlations that were developed from AP600 test data are valid for the AP1000 PRHR and design changes should provide increased safety margin for non-LOCA decay heat removal transients compared with the AP600.

4.3.2 Scaling Analysis

632 Clearly, the applicability of the AP600 tests for validating the LOFTRAN model of the PRHR is of fundamental importance to the AP1000 safety case. It is therefore necessary to examine how well the tests used to validate the code scale to the reactor conditions. Westinghouse and US NRC (Refs 53, 56 and 57) have invested considerable resources in developing test facilities to validate the performance of the passive systems on AP600 and AP1000 based upon scaling criteria for single phase and two-phase flow around loop circuits during natural circulation conditions. These scaling criteria are derived using similarity criteria that are based upon the conservation equations for mass (continuity equation), momentum and energy, the boundary conditions, and the geometry of the system including integral balances around entire loops. Such analysis for natural circulation conditions is made more complicated because of the coupling of the driving force and the heat transfer processes.

633 In practice, for single phase flow, if the natural circulation flow represents an approximate steady-state condition and the pressure (and coolant) used in the test facility are identical to those in the reactor then the similarity conditions (or scaling groups called π groups) simplify (Ref. 56) such that providing the elevation of the driving head is identical, and the flow resistances around the loop and the power of the facility are appropriately scaled, then the physical phenomenon measured on the facility should be well scaled. The results can then be used to support code validation. It should be noted that for the vast majority of intact circuit faults the primary circuit remains single phase. In the case of two-phase flow, the situation is more complicated in that two-phase multipliers enter into the flow resistance term in the momentum equation and so it is important to ensure the core exit steam quality (X_e) and void fraction of the two phase mixture are well preserved.

634 The PIRT and scaling report (Ref. 53) presents in Tables 5-1A and 5-2A the scale ratios for the core exit quality during steady state two phase natural circulation flow for the AP600, AP1000 relative to SPES and Oregon State University (OSU) test facilities. These tables illustrate that the scaling ratios for the SPES-2 facility are close to 1.0 and so Westinghouse have concluded that the facility is well scaled for both the AP600 and the AP1000 for natural circulation conditions. The SPES-2 facility was designed to model the AP600 plant at full elevation and full pressure while simulating the AP600 power

range with a volume scaling factor of 1/395. All the main coolant loop piping and passive safety systems were expressly designed in order to represent the AP600 plant. In contrast, the OSU facility is not well scaled for pressurised natural circulation flow conditions on either AP600 or the AP1000. Westinghouse argues that the distortion on the OSU facility is largely associated with the PRHR flow path resistance which is too high and results in a very high core exit quality.

635 The evidence provided by Westinghouse to demonstrate that the SPES-2 facility is well scaled for full pressure natural circulation conditions supports a conclusion (significant in my opinion) that the SPES-2 facility test results can be reasonably read across to give predictions for AP600 and AP1000 without the need to use computer codes such as LOFTRAN to interpret and scale the results. Nevertheless, there are complications. The scaling ratios assumed steady state conditions. In addition, the much smaller size of the SPES-2 test facility (1/395) means that the effects of wall heat losses and extra metal mass will be greater than on a reactor because of the test facility's relatively larger stored energy, and the surface-to-volume and metal-to-fluid ratios: this will affect the response, although the post-trip input power level was adjusted based on heat balance measurements to account and correct for these effects.

636 Additional comfort can be drawn from the fact that a test of the functionality of the PRHR will be performed as part of the hot functional tests during station commissioning prior to fuel load. Furthermore, Westinghouse is proposing to functionally test the PRHR in the low-power test phase of the commissioning programme for the first AP1000 plant to be built in China. I have raised an Assessment Finding, **AF-AP1000-FS-18**, for a future licensee to analyse the results of these tests when they become available and to demonstrate that the performance of the PRHR is consistent against predictions based upon the scaled experimental tests and the computer codes validated against them.

4.3.3 Experimental Test Programme

637 The results of the SPES-2 tests are reported in detail in the final data report (Ref. 54) and the final test analysis report (Ref. 55). The results are compared with LOFTRAN predictions of the same transients in the AP600 LOFTRAN verification and validation report (Ref. 42).

638 None of the SPES-2 tests specifically studied loss of feed faults. However, three SGTR fault tests (Tests 9, 10, 11) were performed. Test 9 modelled the operation of the control systems and the active safety systems on the AP1000 while Test 11 modelled operator initiation of ADS. Test 10 relies only upon the passive safety systems to cope with the fault. SGTR faults are discussed in more detail in Section 4.2.8 below but the main aim of the analysis is to ensure that the SG will not become liquid-solid (overfill) and that the primary and secondary pressures are brought into equilibrium, terminating flow through the break. It is also the design intent that CMT level should not drop to a point that automatic depressurisation is initiated. In SGTR faults, the break flow though the tube rupture is governed by the difference between the primary and secondary pressure, which in turn is highly dependent upon the cooling to the primary system provided by the PRHR. In my judgement, Test 10 therefore represents a good test of PRHR performance that provides confidence in its ability to perform a similar role for other faults such as the loss of feed and main feed line break faults considered here.

639 The report concludes (Ref. 42) that the LOFTRAN simulation of the test shows good agreement, particularly in predicting the CMT and PRHR behaviour where good to

excellent agreement[1] was obtained. The report also notes that the code model showed little variation in sensitivity studies indicating that the design of the passive systems was robust in single-phase flow conditions.

640 The report (Ref. 42) presents comparisons of code predictions against experimental measurements for primary and secondary pressures, break flow and the integrated break flow mass, hot and cold leg temperatures, pressuriser level, PRHR flow, PRHR inlet and outlet temperature, CMT flow and upper head mass and level. Having studied the results, I agree with Westinghouse that the agreement is good although I note the comparison calculations were not performed blind. The test results and predictions differ from those reported in the EDCD (Ref. 16) for a single SGTR fault. This is because the results reported in the EDCD assume that the CVS remains operational and that pressuriser heaters remain functional: this makes the transient more onerous in terms of margin to overfill since these systems help to hold up the primary pressure and maximise the break flow. The test results show that without these effects the primary pressure falls more quickly, the pressuriser initially empties, and the upper head becomes saturated. Nevertheless, the test results confirm that the CMTs do not enter the drain-down mode following a single SGTR fault.

641 In addition to the integral measurements made on SPES-2 facility, Westinghouse has also performed a series of tests on the stand-alone AP600 PRHR test facility (Ref. 58). These tests aimed at providing design information and data on the heat transfer behaviour of the PRHR covering both forced and natural circulation conditions. They also examined boil-down of the IRWST water level and its effect on the performance of the PRHR. The facility is a full height, full pressure, full temperature facility in which the primary system fluid Prandtl and Reynolds numbers are maintained. The facility consists of three PRHR heat exchanger tubes with the same physical dimensions and pitch as on the reactor design. Heat transfer was measured by recording water temperature at various locations in the tubes, in the walls, and outside in the tank of water including inside the baffle space as well as the main tank volume. A series of configuration tests, plume tests, steady-state tests, transient tests and tests where tubes were uncovered were performed.

642 In analysing the results, Westinghouse assumed that the single-phase forced convection heat transfer coefficients inside the tubes were known (Dittus-Boelter or Petukov-Popov correlations were used depending upon the application that will be made in the safety analysis). Depending upon the wall temperature a combination of natural convection correlations for low temperatures (Eckert-Jackson and McAdams) and pool boiling correlations for higher temperatures were determined from the results of the tests. The standard pool boiling correlations were all found to over-predict heat transfer compared with the test results. This suggested to Westinghouse that strong natural circulation flows occur within the heat exchanger tubes in the IRWST suppressing the onset of boiling. Westinghouse adjusted the Rohsenow correlation by fitting it to PRHR test data that were confidently judged to be in the boiling regime. In practice, Westinghouse conservatively biases the data at the 95% confidence level depending upon the safety analysis application to ensure a conservative result.

643 The semi-empirical approach and the prototypic boundary conditions of the test rig give me confidence in the derived correlations. However, the test consists of only three heat exchanger tubes whereas there are 689 tubes on the AP1000 design, and in scaling up

[1] Westinghouse typically (Ref. 90) defines excellent agreement as the calculated result lies within the uncertainties of the measurements at all times. Good or reasonably agreement is defined as the calculated result sometimes lies within the uncertainties of the measurements and shows the same trend as the data. If these requirements are not met the agreement is regarded as minimal. Inadequate agreement is defined as the code cannot model the phenomena.

from the AP600 to the AP1000 design the horizontal sections of the heat exchanger tubes have been extended. As part of the hot functional testing during the commissioning programme of the first AP1000 reactor to be built, Westinghouse is proposing to perform IRWST heat-up tests using the PRHR as the heat source. This test will measure the vertical water temperature gradient in the IRWST at the PRHR heat exchanger tube bundle and at several distances from the tube bundle. For this reason, Assessment Finding **AF-AP1000-FS-19** has been raised, requiring a future licensee to demonstrate, using these measurements that the performance of the PRHR is consistent against predictions based upon the scaled experimental tests and the computer codes validated against them.

4.3.4 Assessment of the LOFTRAN Computer Code

644 The LOFTRAN computer code (Ref. 120) was developed to simulate the behaviour of multi-loop PWRs with active safety systems during non-LOCA events. The code models the reactor core and vessel, hot and cold leg, steam generator (tube and shell sides), pressuriser, and RCPs. The code and its variants have a long history with the base LOFTRAN code variant being licensed for design-basis non-LOCA analysis by the US NRC in 1983. The capabilities of the LOFTRAN code have been supplemented by the LOFTTR2 code version with SG model developments to provide an improved representation of SGTR fault transients. The LOFTTR2 code variant was licensed by the US NRC for SGTR analysis as discussed in Ref. 84.

645 The base LOFTRAN and LOFTTR2 code variants include models for the active safeguards of earlier plant designs but do not include models to represent the passive safety systems of the Westinghouse AP600 and AP1000 plant designs. These features have been added in more recent parallel code variants LOFTRAN-AP and LOFTTR2-AP which have been used for AP1000 analysis. The code has only limited two-phase flow modelling capabilities, so it can be applied only to intact circuit faults and a limited subset of LOCA analysis calculations which involve zero or very limited levels of primary circuit voidage (i.e. SGTR, feedline break and steam line break faults).

646 While LOFTRAN and LOFTTR2 are old codes and no longer represent ‘state-of-the-art’, both the original codes and updated versions (to include passive features) have been subject to extensive verification and validation. They have also been reviewed and certified by US NRC. While modern codes may be more powerful and flexible, there is no fundamental reason why the predictions made by LOFTTR2 should be invalid providing the transient modelled is covered by the physics and validation of the code.

647 I commissioned AMEC to review the LOFTRAN code and derivatives against the requirements of SAPs FA17 to FA24, including an assessment of validation available to support modelling of the passive systems. AMEC also considered the expectations for validation of computer codes set out in HSE Technical Assessment Guide (TAG) 042 (Ref. 86). AMEC reached following conclusions:

- The LOFTRAN code variants with passive system models are judged adequate for use in conservative assessments of design-basis faults in support of the AP1000 deterministic safety case.
- The LOFTRAN code variants with passive system models are judged to meet the requirements of the HSE Safety Assessment Principles FA 17 to FA 24 at present. This is judged likely to remain the case based on the practices in the Westinghouse Quality Management System.

- Use of an alternative code with more detailed model capabilities would be beneficial to facilitate less conservative assessments for the non-LOCA safety analysis.

648 The use of LOFTRAN for faults presented in Chapter 15 of the EDCD has been assessed by the US NRC, and judged to be acceptable for that purpose (Chapter 21 of Ref. 87).

4.3.5 Findings

649 On the basis of its long history of use, Westinghouse's extensive validation of the modelling of passive systems, AMEC's assessment against FA.17 to FA.24, and US NRC's judgement of its acceptability, I am satisfied with the appropriateness of LOFTRAN for the EDCD design-basis analysis.

650 With respect to my sampling of the validation for the PRHR, SAP EHT.2 states that inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of the heat transport system providing they are shown to be effective in the conditions for which they are claimed. SAPs FA.17 and FA.18 require that analytical models should be validated by comparison with appropriate experiments and tests. In my opinion, subject to satisfactory confirmation from the first of a kind commissioning tests (see Assessment Findings **AF-AP1000-FS-18** and **AF-AP1000-FS-19**), the validation evidence for the LOFTRAN modelling of the PRHR is sufficient to meet these requirements. On the basis of this discussion, I therefore conclude that the requirements SAPs EHT.2 and FA.17 and FA.18 and hence also the requirements of FA.7 have been met.

4.4 Assessment of Validation Evidence for Passive Safety Systems for LOCA faults

651 The safety approach of the AP1000 design to SBLOCA faults is radically different from that on conventional PWRs. The AP1000 plant does not rely on active safety injection pumps to refill the RCS during SBLOCAs, but instead on a range of novel passive safety features to prevent or minimise uncovering of the core. The passive design safety approach of the AP1000 is to depressurise the RCS if the flow from the break is greater than the make-up capacity of the CVS (or the CVS fails). The design intent is for the steam generated by the flashing of the RCS inventory during the blowdown phase to be quickly discharged to containment through the ADS valves. Opening the ADS valves deliberately introduces a large break on the hot leg equivalent in size to a 2A LBLOCA allowing the RCS pressure to fall to a sufficiently low value to allow the introduction of borated water from the IRWST safety injection line into the reactor relying only on gravity.

652 Prior to establishing medium-term injection from the IRWST, safety injection is provided by a combination of the CMTs and the accumulators. As the CMTs are at the same pressure as the RCS and are located at an elevation above the core, natural circulation flow (single phase conditions) or gravity-driven drain-down flow (in two-phase conditions) can be relied upon to provide borated make-up water to the RCS. The accumulators also achieve passive safety injection through the use of pressurised gas. As the pressure in the RCS falls a non-return valve (or check valve) opens allowing pressurised borated water from the accumulator to inject into the RCS. In the long term, as the IRWST drains, the injection source is switched from the IRWST tank to the containment sump where water discharged from the RCS and condensed by the PCS is collected.

653 Given the importance of these passive systems to the safety of the AP1000 design, it is essential that there is high confidence in the functional capability of the CMTs, accumulators, ADS lines, IRWST lines, and recirculation lines to perform their safety

function. It is noted that the PSA (Ref. 36) claims the reliability of these passive systems to be as follows:

- Core Make-up Tanks 1.1×10^{-4} per demand;
- Accumulators 6.9×10^{-5} per demand;
- ADS Stages 1 to 3 lines 5.6×10^{-7} per demand;
- ADS Stage-4 lines 3.1×10^{-5} per demand;
- IRWST lines 6.9×10^{-5} per demand;
- Recirculation lines 1.7×10^{-5} per demand.

654 For this reason, I have chosen to review the test programme performed to support the code validation work for the passive core cooling systems. In particular, I have sampled the following areas:

- the sizing decisions of Westinghouse;
- the scaling analysis of the test facilities;
- relevant experimental test programmes, and;
- the validation of the NOTRUMP and WCOBRA / TRAC computer codes.

4.4.1 Component Sizing

655 The following sub-sections discuss the implications of Westinghouse's sizing decisions on the performance of the CMTs, accumulators, ADS vents and the IRWST / containment recirculation injection lines.

CMT Sizing

656 With regard to the sizing and performance of the CMTs, the PIRT and scaling report (Ref. 53) notes the following points.

- The reactor thermal power has increased by 73% in going from AP600 to AP1000.
- The flow resistance of the orifice in the line between the CMT outlet and the DVI nozzle has been reduced by 64% in going from AP600 to AP1000. This is sufficient to increase the injection flow rate during drain down by 25%.
- The size of the CMT tank has also been increased by 25%. This size determines the mass of water stored and hence the time to reach the ADS Stage-1 to 3 and Stage-4 actuation level set-points. The increased size compensates for the increased flow to maintain roughly the same timings for actuation of ADS.
- The elevation of the top and bottom of the CMT and the DVI nozzle are the same.
- With regard to the sizing of the CMT, the increase in the reactor power and RCS inventory provides extra margin for a given break size because it takes longer for the mass inventory to reduce and the amount of sensible heat is proportionally smaller so the CMT flow rate does not have to necessarily scale with power.

657 The PIRT and scaling report (Ref. 53) acknowledges that the increase in CMT flow by 25% is not sufficient to maintain the safety margins that were available on the AP600 and that the limiting case for CMT sizing is the DVI line break with failure of the intact accumulator.

658 A study of the Westinghouse CMT sizing calculation note (Ref. 91) confirms that the limiting fault for CMT sizing is the DVI line break with a passive single failure of the accumulator check valve on the intact loop, a sequence that I required Westinghouse to analyse with NOTRUMP in its response to RO-AP1000-47 (Ref. 32) on passive single failures as discussed in Section 4.2.8.5 above. The design intent is that the CMTs should be sized to inject for 20 minutes; by this time it is assumed that ADS will have depressurised the RCS so that IRWST injection can commence. Ref. 91 notes that a short time without injection is acceptable providing the core is not uncovered. This is a key ALARP decision that takes no account for example of the 30 minutes rule in SAP ESS.8. A series of sensitivity studies is presented to determine the optimum sizing. In one case the CMT injection flow is increased (through the use of a larger orifice) and the CMT is made larger in proportion to the power up-rating from AP600 to AP1000 so that the margins and timings remain unchanged from AP600. This case is rejected because the CMT has become so large that it becomes virtually spherical which the report states would be very expensive to manufacture.

659 After the DVI line break, the next most limiting fault transient is during shutdown conditions once the accumulators are isolated. In contrast, in the case of the LBLOCA fault at power the flow from both CMTs is available so the calculation note judges that there is plenty of margin available.

Accumulator Sizing

660 Specifically with regard to the sizing and performance of the accumulators, the PIRT and scaling report (Ref. 53) notes that:

- the reactor thermal power has increased by 73% in going from AP600 to AP1000;
- the sizing of the accumulators is unchanged from the AP600 design, and;
- the peak clad temperature increases pro-rata with peak linear rating (which is less than the increase in reactor power because of the switch to 14 ft (4.27 m) fuel) and the time at which the core is uncovered.

661 The report acknowledges that the margin to safety for the LBLOCA has been reduced in going from AP600 to AP1000. It also notes that for a given size of accumulator increasing the flow rate by altering the limiting flow orifice in the discharge line would shorten the duration of injection which is not desirable. Clearly increasing the size or number of the accumulators would have implications for plant layout.

662 The accumulator sizing calculation note (Ref. 92) confirms that there is adequate margin with the AP600 accumulator design. It performs some simple calculations to determine the required orifice size on the discharge line based upon an assumed depressurisation transient as an input boundary condition. The note also states that the design-basis sizing criterion for the accumulators on the AP1000 is the 2A LBLOCA fault with both accumulators assumed to be available. The sizing criterion for the accumulators for the PSA is the 2A LBLOCA fault with only one accumulator assumed to be available. As Westinghouse considers the 2A LBLOCA to be within the design basis it has been required during Step 4 of GDA to consider the 2A LBLOCA with failure of an accumulator as a design-basis fault and perform revised safety analysis. The assessment of this revised analysis is reported in Section 4.2.8.8 above.

ADS Vent Sizing

663 Specifically with regard to the sizing and performance of the ADS vent lines, the PIRT and scaling report (Ref. 53) notes that:

- the reactor thermal power has increased by 73% in going from AP600 to AP1000, and;
- the diameter of the ADS Stage-4 lines has been increased to reduce the overall flow resistance by 28%. The vent area has increased by 76% in line with the power increase although the effect of velocity head during critical flow would be to reduce the effectiveness of this. The non-choked flow will increase by 189%: this is the more important phase to ensure IRWST injection. This is greater than the increase in power ratio.

664 The report concludes that the ADS should provide increased margins relative to AP600.

665 During hot functional testing of the first AP1000 to be built, Westinghouse is proposing that two blowdown tests of the RCS should be performed using the ADS valves. The first would be performed using the ADS Stages 1-3 valves. The second would be performed using a single ADS Stage-1 valve together with a tripping of the RCPs and injection from the CMTs to drain down to the ADS Stage-4 valve actuation set point. Given the importance of these components, Assessment Finding **AF-AP1000-FS-36** has been raised for a future licensee to analyse the results of this test to confirm that the performance of the ADS vents and the CMTs are as expected and that the spargers are able to adequately limit loads on the IRWST.

IRWST / Recirculation Injection Line Sizing

666 With regard to the sizing and performance of the IRWST and containment recirculation lines, the PIRT and scaling report (Ref. 53) notes that:

- the reactor thermal power has increased by 73% in going from AP600 to AP1000;
- the diameter of the injection lines has been increased from 6 inch (15 cm) to 8 inch (20 cm) such that the flow resistance of the IRWST injection line has decreased by more than a factor of 3;
- the level of the IRWST has been increased resulting in an increase in the pressure head by 108%;
- the IRWST flow rate has therefore increased by 184%, and;
- the diameter of the recirculation lines is identical to the IRWST injection lines and so the flow resistance of the recirculation lines has decreased by more than a factor of 3.

667 The report notes that the capability of the IRWST lines and the containment recirculation lines has been increased on the AP1000 design relative to the AP600 design.

4.4.2 Scaling Analysis

668 The PIRT and scaling report (Ref. 53) divides a SBLOCA transient on the AP1000 into seven distinct phases. These are as follows:

- blowdown;
- natural circulation;

- ADS Stages 1-3 automatic depressurisation;
- CMT injection;
- ADS Stage-4 automatic depressurisation;
- IRWST injection, and;
- long-term containment recirculation injection.

669 Westinghouse argues that the initial blowdown phase of the transient is essentially identical to a conventional PWR since none of the passive systems on the AP1000 design will have much effect on this phase of the transient until the RCS has depressurised to the saturation conditions defined by the secondary side pressure in the SGs. For SBLOCA most of the reactor inventory remains inside the RCS.

670 The scaling during the natural circulation two-phase flow has already been discussed in Section 4.3.2 concerning PRHR validation.

671 For other phases, the situation is more complex since the system pressure is reducing with time. The key factor is the fractional rate of pressure change and whether this is dominated by steam production due to decay heating or by the discharge of steam associated with the vent path flow. This is determined using the system-level equations (conservation of mass, momentum, and energy).

672 The equations are combined to reduce the number of scaling groups and put in a form that highlights the physical variables such as reactor vessel inventory, pressure, quality, or void fraction. Simplifying assumptions are made to achieve this goal. The equations are then non-dimensionalised using reference values such as an initial conditions or a steady-state value. The resulting dimensionless coefficients in the equations are normalised using one of the coefficients in the equation. Generally, the coefficient associated with the most dominant process is chosen.

673 From these equations, the ratios of dimensionless π-groups, time constants (τ), or frequencies (ω) (for transient equations where $\omega = \pi/\tau$), are obtained by comparing test facilities and plant scaling ratios. The frequency is the ratio of the rate of transfer of a conserved property relative to the capacity of the receiving volume or mass. It can also be interpreted as the fractional rate of change of the receiving volume or mass by the transfer process. Higher frequencies represent stronger coupling. It is the goal of scaling to preserve higher-frequency processes between a scaled test facility and the plant.

674 During the later phases of the SBLOCA transient (IRWST injection and long-term containment recirculation injection) the RCS pressure stabilises and core exit quality again becomes the key scaling parameter for integral comparisons.

675 For each of these phases, the PIRT and scaling report (Ref. 53) presents in Tables 5-1A and 5-2A the scale ratios for the core exit quality for two-phase “steady-state” conditions and the fractional rate of change of pressure for two-phase “transient” conditions for the AP600, AP1000 relative to the SPES and OSU APEX test facilities. These ratios are the key system-level scale ratios for each of the different phases of a SBLOCA fault. The tables illustrate that the scaling ratios for the SPES-2 facility are close to 1.0 during the natural circulation phase of the transient as expected from the earlier discussion on the PRHR in Section 4.2.3.3 above. The tables also demonstrates that the relative contributions to the rate of change of pressure from steam generation and from ADS venting are similar during the initial ADS Stage-1 to 3 depressurisation phase for the SPES-2 facility. The APEX facility is not well scaled during these early phases of the transient.

676 As the RCS pressure falls, both facilities are seen to be well scaled during the CMT injection phase, which is important for determining the actuation time for the ADS Stage-4 valves. This is probably not surprising as the injection flow rate is determined by the drain-down equation which is governed by the DVI line resistance and the height of the water level in the CMTs.

677 Once the ADS Stage-4-valves actuated the RCS pressure falls rapidly. The SPES-2 facility was not designed for such low pressures. As the pressures fall the flow through the ADS Stage-4-valves becomes non-critical and the line resistances become important. The scaling report acknowledges that for SPES-2 the ADS Stage-4 lines resistances are oversized and so the scale ratio for ADS Stage-4 vent flow becomes distorted at 6.5 for AP1000. Its core exit ratio also becomes highly distorted and it is not able to represent the long-term recirculation phase.

678 In contrast, the APEX facility was specifically designed to test the low pressure long-term injection phase. The APEX facility models the AP600 plant at ¼ elevation length-scale and its maximum pressure is only 27.5 bara with a diameter scaling 0.1443 for vertical pipes and 0.1612 for horizontal pipes. To shorten the time frame for the long-term tests, the facility was deliberately designed to have time scaling factor ½. The low initial pressure, the ¼ elevation height and the time scaling makes its scaling analysis more complex: not all features can be accurately scaled. The aim is to ensure that the key PIRT phenomena are well scaled. The design of the facility is discussed in a peer-reviewed journal article (Ref. 57). Given the time scaling, the facility is well scaled if the fractional rate of change scale ratio is about 2.0.

679 The results in the Table 5-1A of the scaling report (Ref. 53) illustrate that the scaling ratios for the APEX facility are close to 2.0 during the ADS Stage-4 blowdown phase and the subsequent transition to IRWST safety injection and long-term recirculation injection phases.

680 The evidence provided by Westinghouse suggests that the SPES-2 facility is well scaled for full pressure conditions while the OSU APEX facility is well scaled for low pressure conditions after the ADS Stage-4 valves have opened. This is a very useful result since it suggests the two test facilities complement each other by ensuring adequate validation evidence over the full range of conditions modelled by the tests. Additional comfort can be drawn from the fact that tests of the ADS blowdown and CMT drain-down will be performed during the hot functional testing of the first reactor to be built. Assessment Finding **AF-AP1000-FS-36** has been raised for a future licensee to analyse the results of this test to confirm the performance of the CMT is within the assumptions made in the safety case.

4.4.3 Experimental Test Programme

681 The validation evidence of the NOTRUMP and WCOBRA / TRAC computer codes for applicability to LOCA faults on the AP1000 is summarised in the AP1000 code applicability report (Ref. 52). As with non-LOCA faults, there are two steps to the validation argument. The first step of the argument uses the AP1000 PIRT and scaling assessment report (Ref. 53) to argue that the operating conditions and the PIRT assessment developed for LOCA events on AP600 remain applicable after taking into account the increased component capacities on the AP1000 to accommodate and compensate for the higher core power rating. The AP1000 code applicability report (Ref. 52) therefore argues that the validation tests performed for the AP600 remain appropriate for AP1000.

682 The second stage of the argument uses the supporting references to the NOTRUMP final validation report for AP600 (Ref. 90) and the WCOBRA / TRAC applicability to AP600 LBLOCA report (Ref. 104) to justify the validation for AP600. With regard to the performance of the passive systems, the main references are the APEX test reports performed at OSU by Westinghouse (Ref. 93) and US NRC (Ref. 94), the SPES-1 and SPES-2 tests (Refs 54 and 55) already discussed for non-LOCA faults, and the separate effect AP600 CMT test data report (Ref. 95). It is noted that US NRC also performed some independent tests at the ROSA facility in Japan (Refs 96 and 97).

683 The results of the Westinghouse APEX tests are reported in detail in the final data report (Ref. 93). The results of these APEX tests, together with those from SPES-2 tests and other separate effect tests, are compared with NOTRUMP predictions of the same transients in the final validation report for AP600 (Ref. 90). The results from seven APEX SBLOCA fault tests (Tests SB9, SB10, SB12, SB13, SB14, SB18, and SB23) and the six SPES-2 SBLOCA fault tests (Tests S00303, S00401, S00605, S00706, S00908 and S01007) are compared with NOTRUMP predictions. I have chosen to sample:

- Test SB12: this is a DVI line break which relies upon the passive systems to cope with the fault with a failure of one ADS Stage-1 valve and one ADS Stage-3 valve, and;
- Test S000706 which is also a DVI line break with the same single failures.

In my judgement, these tests should be reasonably representative of the performance of the passive core-cooling system and should provide confidence in its ability to perform a similar role for other SBLOCA faults.

684 The report (Ref. 90) presents comparisons of code predictions against experimental measurements for a comprehensive range of parameters including primary and secondary pressures, pressuriser level, break mass flow, core mixture levels, CMT mass flow and level, accumulator mass flow, IRWST mass flow, ADS mass flow, DVI line mass flow, core mass flow, core inlet and outlet temperatures, PRHR mass flow, PRHR inlet and outlet temperature. The report concludes (Ref. 90) that the NOTRUMP simulation of the tests shows reasonable agreement recognising that the calculations are biased to be conservative. However, it concedes that agreement on core mixture level between 140 and 400 seconds on the APEX test and between 200 and 800 seconds on the SPES-2 tests is minimal with the code predictions being non-conservative. Having studied the results, I agree with Westinghouse that the overall agreement is reasonable given that all the other parameters are reasonably well predicted although noting that the comparison calculations were not performed blind. However, given that the time-scale factor of 2.0 and the height factor of 4.0, the agreement between the two test facilities designed to operate at different scales and with different pressures is very good. Importantly, both the tests and the code predictions suggest that the core is fully covered by water or a two-phase mixture during the transient. I have also compared the results of this test with US NRC APEX test NRC-AP1000-01 results for a DVI line failure assuming the failure of all the ADS 1-3 valves (Ref. 94). The results of the test look qualitatively similar although the scales in the US NRC report have been made dimensionless making comparison difficult. The test results again suggest that the core is fully covered by water or a two-phase mixture with no heater rod high-temperature excursion during the entire test in a transient that is more onerous than the Westinghouse tests.

685 In addition to integral measurements made on SPES-2 and APEX facility, Westinghouse has also performed a series of tests on the stand-alone AP600 CMT test facility (Ref. 95) aimed at simulating the thermal-hydraulic phenomenon that will occur on the plant over a wide range of representative pressures and temperatures. The facility has also been

used to test the resistance temperature detectors used for the CMT level instrumentation. The facility is half-scale in height and 1/7.8 scale in diameter. It consists of a single CMT tank which is provided with a steam / water reservoir below the CMT to permit gravity drain and simulates the AP600 RCS in that it provides a source of steam and water to the CMT and a storage area for water drained from the CMT. A CMT inlet steam distributor enables either single phase (steam) or a two-phase mixture taken from the reservoir to be injected at the top of the CMT to simulate the cold-leg balance line. A steam accumulator provides additional steam and is provided with a pressure control valve. Pressures, temperatures and flow rates can be measured at various locations around the facility. The test performed included: a series of configuration tests; steam injection tests (to measure condensation on cold steel walls with and without condensables present); steam / water interaction and drain-down tests at constant pressure and decreasing pressure, and with an initial recirculation phase followed by drain-down; and depressurisation tests.

686 In my opinion, the approach gives some confidence in the test data for the purposes of code validation given the prototypic pressures and temperatures. It is recognised that the facility is not full scale. However, during hot functional testing, Westinghouse is recommending that recirculation flow tests of the CMTs should be performed. For this reason, Assessment Finding **AF-AP1000-FS-37** has been raised for a future licensee to analyse the results of the recirculation tests to confirm that the performance of the CMTs is as expected. This test is complemented by the ADS Stage-1 blowdown test with drain-down of the CMTs discussed above, for which Assessment Finding **AF-AP1000-FS-36** has been raised.

4.4.4 Assessment of the NOTRUMP Computer Code

687 Westinghouse's standard code for assessing SBLOCA faults is NOTRUMP. Although it is an old code and no longer represents the "state-of-art", it has been subject to extensive verification and validation. The code was used as part of the original licensing of Sizewell B and assessed by HSE at the time (Ref. 145).

688 Modifications were made to the code to model the passive systems provided for AP600 reactor design. The resulting code was validated against a test database and subsequently approved by US NRC for performing conservative design basis analyses of SBLOCA events. Westinghouse identified no new phenomena in SBLOCA events for the AP1000, when compared to the AP600, and assumed that the test data base was applicable to AP1000.

689 Westinghouse recognise that NOTRUMP has a limited capability for modelling upper plenum and hot leg entrainment, and that it does not predict adequately the core collapsed[1] level during the accumulator injection phase. This is taken into account in the EDCD analysis of SBLOCA.

690 I commissioned GRS to review the available experimental data (both AP600 and AP1000), in particular the SPES-2 and Oregon State University APEX test data, and to review the adequacy of the NOTRUMP predictions and validations presented by Westinghouse. In its report (Ref. 26), GRS observed that the NOTRUMP predictions of a number of physical tests conducted on SPES-2 and APEX were in poor agreement with the empirical results but that NOTRUMP was always conservative.

[1] Collapsed level refers to what the water level in the core would be if the saturated two-phase mixture in the core were to be separated out into liquid and vapour phases.

691 Given their novelty and their importance to the PXS, GRS chose to take a closer look at the modelling of the CMTs. The NOTRUMP model of the CMT consists of four fluid volumes: the upper volume is important because the incoming hot fluid interacts with the CMT water which is subcooled at the start of a fault transient. In its report (Ref. 26), GRS questions whether the NOTRUMP model of the CMT is able to represent all the potential phenomena: this could be a cause of some of the divergence between predictions and test results. For this reason, GRS chose to focus on the performance of the CMTs during its review of potential failure modes discussed in Section 4.5 below.

4.4.5 Assessment of the WCOBRA / TRAC Computer Code

692 The WCOBRA/TRAC computer code has been developed to represent the main phenomena occurring in a LBLOCA on the basis of integral models of flow and heat transfer. These models capture the global characteristics of the flows using plausible physics, based on empirical data.

693 In accordance with the formal process set out by the US NRC (Ref. 105), Westinghouse has assessed the issues of scaling between the size of the tests used to derive the models and the size of the reactor. This has been reviewed by the US NRC and found to be acceptable (Ref. 103). HSE has previously reviewed the WCOBRA / TRAC computer code since it was used for the modelling for Sizewell B (Ref. 145).

694 The validation of the modelling has followed a systematic, targeted approach based on the ranking of phenomena according to their significance and the use of both separate-effect and integral testing. This follows a standard approach to ensure that significant modelling parameters receive due consideration.

695 The US NRC assessment reported in Ref. 107 concluded that Westinghouse had conservatively calculated, bounded, or directly included all the appropriate items in the methodology. The rigour with which uncertainty in parameters, such as blowdown heat transfer coefficients, are substantiated is impressive. The qualification documents run to thousands of pages.

696 Plant operation, geometric and modelling uncertainties are all represented on a realistic basis in a Monte-Carlo study. The exception is the modelling of the entrainment of water droplets out of the reactor vessel, where a modest conservatism in the modelling is accepted.

697 Nodalization has been studied. Westinghouse has not attempted to refine the model, but has compared the nodalization of the AP1000 model with that of integral test facilities used in the code qualification. This is the general practice for primary-circuit models of this kind.

698 I examined the formulation of the numerical methods and I noted that the frictional resistance to flow in the direction perpendicular to the axis of a flow channel in the core was formulated relatively crudely. I required a sensitivity study be made with a more detailed formulation. I am satisfied that this issue does not introduce significant error into LOCA predictions.

699 I conclude that the WCOBRA / TRAC code qualification appears to be a comprehensive piece of work and that the code remains fit for purpose.

4.4.6 Findings

700 SAP EHT.2 states that inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of a heat transport system providing

they are shown to be effective in the conditions for which they are claimed. Additionally, SAPs FA.17 and FA.18 require that analytical models should be validated by comparison with appropriate experiments and tests. In my opinion, subject to satisfactory confirmation from the first AP1000 commissioning tests, the validation evidence for the NOTRUMP and WCOBRA/TRAC modelling of the CMTs, accumulators, ADS vents, IRWST and recirculation injection lines meets these requirements. On the basis of this discussion, I therefore conclude that the requirements of SAPs EHT.2, FA.17 and FA.18, and hence also of SAP FA.7, have been met.

4.5 Review of Thermal-Hydraulic Failure Modes on the Passive Safety Systems

701 The passive systems have relatively few moving parts so that their conventional reliability, as typically presented in a PSA in terms of the failure probability of a component to operate, is likely to be impressive. However, it must be recognised that confidence in their ability to function is only as good as the confidence in the thermal-hydraulic analysis performed to justify their functional capability. The thermal-hydraulics of two-phase flow can be very complex. For example, the performance of natural circulation flow can be significantly affected by the following phenomena:

- interaction among parallel loops;
- engineering uncertainties, i.e. deviation from the “ideal” design (including ageing effects);
- effect of non-condensables;
- stability;
- reflux condensation;
- two-phase flow friction, and;
- co-current and counter-current flow.

702 The phenomena relevant to the performance of gravity-driven draining are:

- temperature stratification;
- screen clogging;
- pressure drop/head losses, and;
- counter-current flow.

703 For this reason, I have contracted GRS to perform an independent review to identify potential thermal-hydraulic failure modes on the AP1000 passive systems. GRS has reviewed this list of potential failure modes against the experimental test results performed at SPES-2 (Ref. 55); OSU (Refs 93 and 94), and ROSA (Refs 96 and 97), and the validation calculations performed using NOTRUMP (Ref. 90). GRS has concluded that of the phenomena listed above (Ref. 26) the following needed to be explored further:

- condensation effects in the CMTs;
- waterhammer effects in the CMTs;
- non-condensable effects on the performance of the CMTs;
- uncovering of core during transition to IRWST injection with two ADS Stage-4 valve failures;
- thermal stratification effects in the core;

- oscillations in injection line flows;
- oscillations and chugging effects on the IRWST, and:
- sump clogging.

704 I commissioned GRS to perform a more detailed review of these phenomena with the exception of sump clogging. As noted in Section 4.2.8.8 above, this has already been thoroughly assessed by US NRC (Ref. 107). The findings of the GRS review are presented in the following paragraphs.

The Effects of Condensation on the Performance of the CMTs

705 In ROSA tests AP-CL-08 and AP-PB-01 (Refs 96 and 97), GRS noticed that the pressure in the CMT fell, causing the CMT to refill. In the second test, the pressure decrease was sufficient for the CMT to completely refill. It should be emphasised that in both cases the CMT subsequently recovered and resumed normal operation. The effect is thought to be due to cold water entering the CMT resulting in higher condensation levels causing the pressure to decrease. Given that the level in the CMT tank is the key parameter used to actuate the ADS valves, it is clearly important that the thermal-hydraulic performance of the CMTs is well understood. Westinghouse stated that such an effect was never seen at the SPES-2 and APEX facilities which are more representative of the AP1000 design.

706 Given these observations, GRS recommended studying the effect of the heat capacity of the CMT structure since this may have an important effect on the operation of the CMTs: the large-scale AP1000 CMTs may well behave differently from ROSA facility. For this reason, GRS was requested to perform a series of single-parameter sensitivity studies using the ATHLET system model of the AP1000. The sensitivity studies looked at the effects of: (i) varying the CMT wall heat transfer coefficient; (ii) inclusion of a flange in the thermal capacity of the CMT vessel (as was the case on ROSA); (iii) a higher surface-to-volume ratio (also consistent with ROSA); and (iv) initial CMT temperature. The results of the analysis performed by GRS (Ref. 27) demonstrate that the dominant effect is the surface-to-volume ratio of the CMT, which on ROSA is much larger than on AP1000. With the ROSA surface-to-volume ratio, GRS was able to replicate the CMT refill event seen in the ROSA test for the 1 inch (2.54 cm) cold leg SBLOCA transient almost exactly. GRS has confirmed that for the AP1000 CMTs these effects are only of minor importance.

Potential for Water Hammer in the CMTs

707 The water and steam mixture in the CMTs becomes stratified during operation. There is normally a layer of hot steam at the top and sub-cooled water at the bottom, with a layer of saturated water in between. GRS is aware of standalone CMT tests (not AP1000 specific) performed at the PACTEL facility (Ref. 27). Here the saturated layer was missing, resulting in condensation of steam on the surface of the sub-cooled water in the CMT. In such circumstances there is the possibility of water hammer in the inlet line at the top of the CMT. Westinghouse stated that no water hammer had ever occurred on any integral test and that there is a sparger on the inlet pipe to the CMT to avoid this problem. GRS was content with the answer (Ref. 27), recognising that the possibility of high pressure pulses is low because there are no closed pipe sections present.

The Effects of Non-Condensables on the Performance of the CMTs

708 GRS has questioned whether CMT operation could be affected by nitrogen flowing out of the accumulators. Westinghouse has replied that a negative effect from nitrogen flow has never been observed on any test. On the contrary, nitrogen entering the balance line inlet into the CMT reduces condensation, which is beneficial. Having examined many of the test results, GRS agreed with Westinghouse's analysis (Ref. 27).

Performance of the ADS Stage-4

709 GRS noted that, during the APEX test NRC-AP1000-05 on a DVI line break, the failure of two ADS Stage-4 vents on the non-pressuriser loop resulted in temporary uncovering of the core during the transition to medium-term IRWST injection. While the failure of two ADS Stage-4 valves during the DVI line break is a beyond design basis event, it does illustrate the potentially limited safety margin available for the design-basis single failure of an ADS Stage-4 valve. For this reason, GRS has performed (Ref. 27) some confirmatory analysis for this sequence including a statistical uncertainty analysis. The results are discussed further in the assessment of single failure sequences presented in Section 4.2.8.2.

The Effects of Thermal Stratification on Core Reactivity

710 GRS questioned whether thermal stratification could occur in the AP1000 core following the transition from natural circulation flow through the SG loops to natural circulation flow through the PRHR as the SGs dry out. Based on evidence from ROSA test AP-CL-03, GRS was concerned that cold water from the PRHR could enter the lower plenum unmixed resulting in a cool-down fault. Westinghouse noted that the CMTs will inject highly borated water into the core at the same time; also no such behaviour was observed at the APEX or SPES-2 tests which are closer to the AP1000 design. These tests show that the natural circulation flow from the PRHR is adequate to ensure good mixing in the core. GRS agreed with these arguments (Ref. 27).

The Effect of Flow Oscillations on IRWST Injection

711 GRS noted that in ROSA test AP-CL-03 the injection flow oscillated due to fluctuations in the hot-leg water level. Such oscillations are undesirable on a passive plant where the aim is to align check-valves only once if possible: repeatedly opening and closing them could cause them to fail. Westinghouse argues that the check valves were tested on a prototypic test facility for AP600 and that the check valves open only slightly. No banging was observed. Westinghouse also argues that the check valves in the IRWST injection line are in parallel and not series so there is redundancy to protect against a single failure. This issue is discussed further in the mechanical engineering assessment report (Ref. 133), where Assessment Finding **AF-AP1000-ME-02** has been raised requiring a future licensee to provide the factory and site acceptance testing information for these valves.

Potential for Sparger Interaction in the IRWST

712 The IRWST is an important structural component of the passive core cooling system. During the ADS Stages 1-3 depressurisation phase of the SBLOCA transient, the spargers discharge steam directly into the water inside the IRWST. The water acts as a

suppression pool, condensing and scrubbing the steam to minimise the containment pressure and to reduce radiological releases into the containment vessel. Although it is a passive structure, it is not provided with redundancy or diversity for its safety function as the source of borated water for medium-term safety injection. It is therefore important that operation of the spargers should not result in the failure of the IRWST. GRS has raised concerns about whether the two spargers that discharge into the IRWST could dynamically interact resulting in excessive loading on key components in the IRWST.

713 In its response to TQ-AP1000-1187 (Ref.9), Westinghouse provides an assessment of the loads on the IRWST due to the dynamic effects of a single sparger discharging into the IRWST. However, in my opinion, this does not address the concerns raised by GRS. The response presents a high-level engineering judgement about the dynamic pressurisation forces on the tank without any quantitative analysis to support the arguments. In any case, it focuses on the forces due to a single sparger rather than on the potential for interaction between the two spargers generating chugging and oscillations in the IRWST. As noted above (Section 4.2.8.5), Assessment Finding **AF-AP1000-FS-38** has been raised for a future licensee to assess the potential for an adverse interaction between the two spargers in the IRWST and to confirm that the structural integrity of the IRWST walls and injection lines is assured in such circumstances.

Conclusions from the GRS Review

714 GRS has concluded (Refs 26 and 27) that the phenomena discussed above are unlikely to lead to safety-relevant failure modes on the AP1000 passive core cooling system with the possible exception of interaction between the two spargers affecting the integrity of the IRWST, for which Assessment Finding **AF-AP1000-FS-38** has been raised.

4.6 Radiological Consequences of Design Basis Events

715 Site-specific calculations for design basis radiological consequences are out of scope of GDA. However to gain confidence that acceptable AP1000 site-specific calculations will be possible in the future, it is necessary to know for GDA that radiological consequences predicted for a generic site compare favourably with the established UK limits. For any comparison to be meaningful, the chosen analysis methodology needs to be compatible with that assumed to derive the UK limits. For GDA, I interpret this as “broadly consistent” and some minor differences in approach from that usually seen in the UK are acceptable.

716 SAP FA.7 states that design-basis analysis of fault sequences should demonstrate, so far as is reasonably practicable, that:

- none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactivity are breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;
- there is no release of radioactivity; and
- no person receives a significant dose of radiation.

717 Where releases do occur, then doses to persons should be limited. The numerical targets to be met by design basis faults are set out in Target 4 of the SAPs.

718 The EDCD (Ref. 16) presents a set of AP1000 design-basis fault radiological consequences analyses, calculated following typical US methods and meeting dose limits

prescribed by US NRC. No attempt is made in Ref. 16 to compare against Target 4 or to compare the adopted methodology against the expectations for the UK.

719 RO-AP1000-48 (Ref. 10) was raised at the end of GDA Step 3 which required Westinghouse to recalculate the radiological consequences for design-basis faults using methods and assumptions consistent with relevant UK good practice (Ref. 121) and to explicitly compare the results against the appropriate Target 4 limits. Westinghouse's response to this RO is summarised in Ref. 50. It is Ref. 50 and its supporting references that have been assessed for GDA Step 4, not the analysis in the EDCD.

720 Ref. 50 discusses new analysis undertaken for the following faults:

- SBLOCA;
- LBLOCA;
- Rod Ejection Accident (REA);
- Locked Rotor;
- Main Steam Line Break;
- SGTR;
- Small Line Break Outside of Containment;
- Loss of Offsite Power;
- Single Rod Withdrawal, and:
- Feed-line Break.

721 Westinghouse states that in some cases its analysis differs considerably from that originally presented in the EDCD. This includes making use of the updated dose conversion factors as set out in International Commission on Radiological Protection (ICRP) Publication 60 (Ref. 125).

722 Westinghouse has chosen to use AFCAP thermal-hydraulic results for fault transients, on the basis that they are the most recently completed and reflect the latest design information. This thermal-hydraulic analysis is different from that presented in the EDCD and assessed in GDA Step 4. As has already been stated in this report, the status of the AFCAP work for GDA and its appropriateness for the GDA AP1000 Design Reference Point is unclear. Therefore, in response to Action 1 of **GI-AP1000-FS-02**, Westinghouse needs to clarify exactly what analysis it is submitting for GDA, including radiological consequences analysis, and to demonstrate why it is appropriate for the UK Design Reference Point.

723 Westinghouse concludes that all AP1000 design-basis faults meet the Target 4 BSLs. To achieve this for the SGTR and small-line break faults outside of containment, Westinghouse found it necessary to reduce the Technical Specification primary coolant activity levels for iodine and noble gas activity by a factor of 4 from the earlier values presented in the EDCD. This is a significant outcome of the revised analysis although Westinghouse does not believe the new activity limits will be restrictive in practice.

724 I commissioned AMEC to review the response to RO-AP1000-48 (Ref. 50) against the expectations for UK design-basis radiological consequences analysis as set out in Ref. 4 and Ref. 121. The result of the AMEC's review are summarised in Ref. 122. Amongst the findings and conclusions reached by AMEC are:

- All the design-basis faults now meet the BSL. However, as they are not below the Basic Safety Objective (BSO), they fall into the area where a formal ALARP justification would be expected.
- For some faults, the review of the identified references has highlighted additional conservatisms compared to UK current practice. This may be considered at a later stage of the licensing process.
- The assumptions on chemistry behaviour are basically in line with accepted UK practice. There is some inconsistency in assumptions on chemical speciation between the activity release calculation and the onsite / off site dose calculation. However, the presented dose methodology is relatively insensitive to iodine speciation; therefore, the impact on the reported doses will be small. AMEC recommends that this should be addressed in future site licensing calculations, either by use of an iodine chemistry code or a more extensive justification document.
- In order to demonstrate compliance with the BSL for the SGTR fault with an activity spike initiated by the accident, the Technical Specification limits for noble gases and dose equivalent iodine are reduced by a factor of 4. This assumption is consistently applied in the analysis of other design basis faults. This reduction is an arbitrary value needed to achieve the BSL; however, the resulting limits are broadly in line with generic guidelines (Ref. 123) on primary coolant activity concentrations which may be used in analysis, in the absence of any other information. This should be confirmed in future by additional justification for these Technical Specification limits; e.g., using operational experience on similar plants.
- The accident-initiated spiking model is based on a number of assumptions that effectively maximise the generation rate of iodine. A more realistic spike activity rate could be considered, based on existing operational experience. It is also noted that only iodine is assumed to spike; in current UK PWR methodologies caesium is also assumed to spike (but noble gases are not).
- The “pre-existing spike” methodology for the SGTR fault does not have any spiking source term. What it represents is a fault occurring when the RCS activity concentration is at the maximum allowed Technical Specification value at a time when there is no enhanced input from the fuel to the RCS; i.e., the appearance rate is the equilibrium appearance rate
- The fuel failure assumptions for the LOCA and REA are reasonably consistent with generic recommendations (Ref. 124); however, there should be additional design-specific justification based on clad damage analysis. The magnitude of the fission product release from failed fuel pins is at the conservative end of the recommended range.
- The Westinghouse methodology excludes the ingestion exposure pathway completely. Although the ingestion dose is expected to be limited, it should be assessed in some way in order to be compliant with Ref. 121.
- For future site licensing, it may be desirable to calculate all off-site doses using a dedicated dispersion and dose code. This is in line with current UK practice and would result in fully verified results for all exposure pathways: inhalation, cloud doses, ground doses and ingestion doses (which have not yet considered for UK AP1000).

725 Through my own assessment of Ref. 50 and the AMEC’s review (Ref. 122), I am satisfied that it should be possible for future site-specific analysis of design basis faults to show compliance with Target 4 of the SAPs.

726 While new site-specific calculations have always been envisaged, I am still raising an Assessment Finding for site-specific design basis radiological consequences analysis to be performed, taking due cognisance of usual UK methodology assumptions and explicitly comparing against Target 4.

727 It is important to reiterate that Ref. 4 states that, while it is HSE's policy that a new facility should at least meets the BSLs, this does not necessarily make the risk ALARP. The application of ALARP may require further measures to reduce the consequences of design-basis faults.

728 While the assumptions made in the new radiological consequences analysis generally appear sensible and conservative (and therefore appropriate for GDA), some of them are rather arbitrary, inconsistent, or yet to be justified. The primary circuit activity Technical Specification limits cited by AMEC are an example of this. These shortfalls will need to be addressed in future site-specific calculations to allow judgements to be formed on whether the risks could be reduced further. For this reason, I have raised Assessment Finding **AF-AP1000-FS-46** requiring a future licensee to perform design basis site-specific radiological consequence analysis taking due cognisance of UK methodology assumptions and explicitly comparing against Target 4 of the SAPs.

729 AMEC's comment on fuel failure assumptions for LOCA is consistent with my own findings set out Section 4.2.8.5 above. The assumption of 10% fuel damage due to DNB for SBLOCA seems sensible but future calculations need to identify for which SBLOCA faults it is assumed to be appropriate or bounding. Also there is a need to establish the summed initiating event frequency for those faults, to justify the level of damage for those grouped SBLOCA faults, and to compare the resulting radiological consequences analysis against the appropriate Target 4 limit.

730 Due consideration should be given to establishing the limiting single failure in the assessment of design-basis radiological consequences. The current analysis reported in the EDCD makes assumptions about single failures in the radiological consequences analysis that are consistent with the assumptions in the design-basis thermal hydraulic analysis. As the radiological consequences methodology for the UK evolves, it will be necessary to check that previous assumptions on limiting single failures remain appropriate. For example, in EDCD radiological consequences analysis for SGTR faults, 100% of the iodine transferred from the primary circuit to the secondary side is assumed to be in the flashed steam mass. Therefore, the limiting transients are likely to be those which maximise the cumulative flashed steam mass through the break. In the new UK analysis reported in Ref. 50, only a small fraction of the iodine in the water transferred through the break is assumed to be released to the SG vapour space and discharged during the flashing phase. Hence, in the updated Westinghouse methodology, the iodine associated with the flashed fraction is less important while the total primary to secondary flow is more significant. Additional sensitivity cases should be performed as part of any site licensing submissions to establish what is the limiting fault sequence to consider in the both the thermal-hydraulic and radiological consequences analysis.

731 As was stated in Section 4.2.12, Westinghouse needs to provide further discussion on the radiological consequences of shutdown faults as part of the response to GDA Issue **GI-AP1000-FS-07**.

732 In addition to the Fault Studies assessment, HSE-ND has assessed the chemistry methodology and claims submitted by Westinghouse in Ref. 50 and supporting references, choosing to sample SGTR faults in detail. This assessment is reported in Ref. 131. It identifies a number of additional assessment findings which should also be addressed by a future UK licensee in site specific calculations.

4.7 Overall Review of the Design Basis Analysis

733 SAP FA.8 requires that Design Basis Analysis should demonstrate that all design basis initiating events are addressed, all safety functions of the design are identified, that the performance requirements for safety systems are identified and that suitable and sufficient safety systems are provided. Furthermore, SAP FA.9 requires that the design basis assessment should provide an input into the safety classification and the engineering requirements for structures, systems and components performing a safety function. In my judgement, based upon my assessment of the design basis analysis performed by Westinghouse reported above, these requirements have been met apart from those exceptions where GDA Issues have been identified.

4.8 Limits and Conditions

734 SAP FA.9 also requires that the design basis assessment should provide an input into establishing the limits and conditions for safe operation and identifying the requirement for operator actions. In particular, the design basis analysis should provide the basis for determining the safety limits for actuator trip settings and performance requirements for safety systems, the conditions governing permitted plant configurations and the availability of safety systems, and the safe operating envelope defined as operator limits and conditions in the operating rules for the facility.

735 As noted in Section 2.3.6 above, it has been agreed with Westinghouse that it is more appropriate to assess the proposed Technical Specifications during the site licensing process. However, HSE-ND has required that Westinghouse define the process for identifying the limits and conditions that will be incorporated into the Technical Specifications. Its proposals are reported in the responses to RO-AP1000-94 (Ref. 126). The response failed to reflect much of the recent work performed during GDA Step 4 on categorisation and classification in response to RO-AP1000-43 and on diversity in response to RO-AP1000-47. For this reason, Cross-cutting topic area assessment GDA Issue **GI-AP1000-CC-01** has been raised (Ref. 144), effectively requiring Westinghouse to revisit its response to RO-AP1000-94. Nevertheless, the design basis analyses reported in Chapter 15 of the EDCD are reasonably clear in stating what assumptions are made about preventative maintenance (essentially none at power on the passive systems) and single failures within the analysis. In my opinion, it should be relatively straightforward to translate this into the Technical Specifications during the site licensing process for at-power reactor faults.

736 In contrast, the work performed on diversity in RO-AP1000-47 tends to assume full plant availability. Given the assumption of common mode failure considered in these sequences associated with frequent initiating events, I believe it is not unreasonable to discount the likelihood of an additional single failure as being outside the traditional UK design basis sequence frequency limit of 1×10^{-7} per year for all but the most frequent of faults. It is less clear whether preventative maintenance work on the active Class A2 systems may also be discounted in this fashion. In practice, this may not be a significant issue for at-power faults as many are ATWT sequences where the DAS has multiple redundancies and preventative maintenance will not be allowed on the passive CMTs. The active cooling systems will need a close review although it is noted that the start-up feedwater system for example is a 2 x 100% system. GDA Issue **GI-AP1000-FS-07** has been raised on this issue in the case of shutdown faults where the position is more complex because it is assumed that some systems will be taken out of service for maintenance.

737 The issue of plant maintenance for both at power and shutdown faults will need to be further reviewed when the Technical Specifications are being assessed during site licensing. It should be noted that there is also scope for technical input from the PSA on these matters.

4.9 Support to the GDA Structural Integrity Assessment

738 As noted in my assessment plan, it was always my intention to assess the thermal hydraulic analysis undertaken in support of the structural integrity assessment of the AP1000 in collaboration with my structural integrity assessment colleagues. In practice, although the design transients have been made available (Ref. 127), Westinghouse is still in the process of carrying out a programme of fracture analysis work to justify claims on defect tolerance of key structural components which may require the revision of some of the key design transients and so it has not proved possible to perform a targeted assessment of these analysis during GDA Step 4. Completion of this programme of work is covered under Structural Integrity topic area assessment GDA Issues **GI-AP1000-SI-01**, **GI-AP1000-SI-02** and **GI-AP1000-SI-04** (Ref. 128). My intention is to assist my structural integrity assessment colleagues with their assessment of the response to these GDA Issues when they become available by performing, on a sampling basis, an assessment of the transient analysis work that is performed to support this work.

4.10 Fault Schedule

739 Discussions have been held with Westinghouse throughout GDA on the requirement for a Fault Schedule for the AP1000. This document should include as a minimum all design basis faults with their initiating frequencies and the safety systems designed to mitigate each fault. Only the “standard” ANSI reactor design basis faults have been considered in Chapter 15 of the EDCD. Westinghouse has been told that all faults meeting the definition of design basis set out in SAP FA.5 (Ref. 4) should be considered, including faults from shutdown reactor states and faults involving the spent fuel pool. The Fault Schedule should also show how diverse means of protecting against frequent faults ($> 1 \times 10^{-3}$ per year) are provided.

740 A comprehensive fault schedule is necessary for visibility to be provided of the safety classification of claimed safety systems providing protection for the fault. This is important as Westinghouse is moving towards the UK safety classification, which is not used in the EDCD.

741 Westinghouse provided a number of draft and provisional Fault Schedules during GDA. However a definitive Fault Schedule, summarising all the safety claims made in the UK AP1000 design basis safety case (including new claims identified in RO responses), was supplied only at the end of GDA Step 4 (as part of Ref. 13). This was too late for assessment within GDA Step4. For this reason, GDA Issue **GI-AP1000-FS-08** has been raised, requiring Westinghouse to provide a Fault Schedule for assessment and provide further substantiation/revisions as required by HSE-ND.

4.11 Initial Test Programme

742 In Chapter 14 of the EDCD (Ref. 16), Westinghouse has outlined its approach to developing the initial test programme for the AP1000. It covers pre-operational testing of Class A1 safety systems, defence-in-depth systems (now Class A2 safety systems), and non-classified systems. Start-up testing will include initial fuel loading tests, pre-criticality

tests, initial criticality tests, low power tests and power ascension tests. The proposed programme has not been assessed during GDA as it is more appropriate to do this as part of the site licensing process. Nevertheless, it has been briefly reviewed in those areas where Westinghouse is proposing to perform tests only on the first AP-1000 plant to be built or the first three AP-1000 plants to be built. It is very unlikely that any of these will be a plant in the UK as four are already at an advanced stage of construction in China and one in the US is at an advanced stage of pre-construction licensing.

743 As noted in Sections 4.2.3.3 and 4.2.8.5 above, as a result of reviewing Westinghouse's proposed initial test programme, Assessment Findings **AF-AP1000-FS-18**, **AF-AP1000-FS-19**, **AF-AP1000-FS-36**, and **AF-AP1000-FS-37** require a future licensee to assess the results of these tests and to confirm that the performance of the passive safety systems is as expected. Alternatively these tests may be performed on the first AP1000 plant to be built in the UK. In addition, in Section 4.2.5.3, Assessment Finding **AF-AP1000-FS-29** has been raised requiring a future licensee to perform a load-follow test during the commissioning for the first AP1000 plant in the UK. In Section 4.2.6.4, Assessment Finding **AF-AP1000-FS-32** has been raised for a future licensee to make proposals covering the commissioning tests for the in-core detectors if the outcome of GDA Issue **GI-AP1000-FS-04** is that these detectors should be connected to a diverse protection system.

4.12 Overseas Regulatory Interface

744 HSE's strategy for working with overseas regulators is set out in Ref. 129 and Ref. 130. In accordance with this strategy, HSE collaborates with overseas regulators, both bilaterally and multinationally. In particular, HSE-ND collaborates through the work of the International Atomic Energy Agency (IAEA) and the Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (OECD-NEA). In particular, the UK is involved in the Multinational Design Evaluation Programme (MDEP). MDEP is a multinational initiative undertaken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. This helps to promote consistent nuclear safety assessment standards among different countries. There have been no MDEP meetings for the AP1000 in the fault analysis area.

745 In the Fault Studies area, a number of bilateral meetings have been held with the US NRC to keep them informed of the fault analysis aspects of the AP1000 GDA. Following on from these discussions, the US NRC has provided access to the input decks for the TRACE and MELCOR computer codes for the purposes of performing confirmatory analysis using TSCs. US NRC has also provided HSE-ND with reports summarising the results and findings of their experimental campaigns investigating AP1000 and AP600 passive systems.

746 HSE-ND is a member of the following OECD nuclear safety research projects:

- The ROSA-2 large scale test facility aimed at supporting research of severe accident phenomena, such as loop circuit thermal stratification and counter current flow.
- The PKL-2 programme looking to provide code validation information on boron dilution and mid-loop operation during refuelling.

747 HSE-ND is also a member of the Code and Maintenance Programme (CAMP) and the Cooperative Severe Accident Research Programme (CSARP) which are aimed at sharing and supporting US NRC code development activities. Both TRACE and MELCOR come under these programmes.

5 CONCLUSIONS

5.1 Key Findings from the Step 4 Assessment

748 In my opinion, Westinghouse has improved the design basis safety case for the AP1000 through the additional analysis performed in response to the ROs raised in my GDA Step 3 report. It has been able to extend the design basis to demonstrate that the design is tolerant to passive single failures at the functional level. Westinghouse has also extended the design basis to cover complex situations in which a combination of events may initiate a fault sequence, although this is an area where there is further work still to be done and a number of GDA Issues has been raised in respect of this.

749 The analytical work performed by Westinghouse has been aided by a number of important design changes to the reactor protection system on the AP1000 that in my opinion will significantly improve the safety of the design. These changes have been proactively identified by Westinghouse. The design changes identified are:

- An upgrading of the following active systems to Category A Class 2 safety systems: the DAS, the SFW system, the RNS system, the CCS system, the SWS, and the stand-by diesel generators. In particular, the RNS system has been upgraded from a single train to a two train system at the point of injection into the DVI lines; the DAS has been upgraded from a 2-out-of-2 to a more fault-tolerant architecture involving a dual 1-out-of-2 and partial 2-out-of-3 system.
- Implementation of a modification to alter the set-point for the isolation the SFW and the CVS on high SG level alarm signal. This will improve protection against a SGTR fault by increasing the margin to overfill on the affected steam generator.
- Implementation of a reactor trip signal on the DAS to trip the reactor on high hot-leg temperature.
- Implementation of a reactor trip signal to mitigate the effects of an inadvertent actuation of the PRHR Heat Exchanger.
- Implementation of a modification to enable the P-17 interlock to prohibit rod withdrawal following a spurious drop fault of one or more rods.

750 In addition, Westinghouse has committed to the implementation of a blocker device on the ADS to reduce the likelihood of a spurious actuation. There is also a commitment to improvements in the design of the spent fuel pool, although the safety cases justifying these design changes have still to be developed.

751 The full list of GDA Issues I have identified during my assessment requiring additional work from Westinghouse is:

- Completion of the safety case is required for the spent fuel pool setting out the claims identified during Step 4 of GDA and providing the supporting arguments and evidence for those claims. The design-change process needs to be followed to incorporate the various physical modifications identified and all the affected documents need to be updated.
- Westinghouse is to demonstrate that, for all design basis faults, the submitted design basis analysis is appropriate for the agreed GDA design reference point, and that all safety claims are supported by the analysis. If this cannot be done with pre-existing analysis, new analysis could be required. The final PCSR produced for GDA is to summarise this analysis for all design basis faults. A complete and consistent set of core design limits reflecting the design basis fault analysis is required.

- Westinghouse to implement design modifications and provide further analysis to demonstrate functional diversity for faults with an initiating frequency greater than 1×10^{-3} per year.
- Westinghouse need to examine the feasibility of enhancing the flux protection on the AP1000 to provide automatic and diverse protection against frequent adverse power distribution faults possibly using the current design of in-core instrumentation.
- Westinghouse is to examine whether it is reasonably practicable to enhance the design of the RNS system in its role as the diverse safety injection system on the AP1000.
- Westinghouse is to provide validation evidence that the IRWST is functionally capable of cooling the PRHR system during intact circuit faults for 72 hours.
- Westinghouse is required to complete a fully integrated design basis safety case for shutdown faults in the PCSR.
- Westinghouse is to present its updated fault schedule.

752 In my opinion, based upon the information provided in the EDCD and supporting documentation submitted as part of the GDA process, there are no fundamental reasons for believing that a satisfactory safety case cannot be made for the generic AP1000 reactor design, subject to satisfactory progression and resolution of GDA Issues during the forward work programme for this reactor. A major item of work will be to assess the revised PCSR. It must also be recognised that some of these GDA Issues may ultimately require changes to the plant design. It is therefore too early to rule out the need for changes to plant layout or the provision of additional safety systems.

5.1.1 Assessment Findings

753 I conclude that the following Assessment Findings listed in Annex 1 should be programmed during the forward programme of this reactor as normal regulatory business.

5.1.2 GDA Issues

754 I conclude that the GDA Issue(s) identified in this report must be satisfactorily addressed before Consent can be granted for the commencement of nuclear island safety-related construction. The complete GDA Issues and associated action(s) are formally defined in Annex 2.

6 REFERENCES

1 *GDA Step 4 Fault Studies Assessment Plan for the Westinghouse AP1000.* HSE-ND Assessment Plan AR 09/048. April 2010. TRIM Ref. 2009/455978.

2 *ND BMS. Assessment Process.* AST/001 Issue 4. HSE. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm.

3 Not used.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.

5 Not used.

6 *Step 3 Fault Studies Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/018. November 2009. TRIM Ref. 2009/335824.

7 *ND BMS. Transient Analysis for DBAs in Nuclear Reactors.* T/AST/034 Issue 1. HSE. November 1999. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast034.pdf.

8 Not used.

9 *Westinghouse AP1000 - Schedule of Technical Queries Raised During Step 4.* HSE-ND. TRIM Ref. 2010/600721.

10 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised During Step 4.* HSE-ND. TRIM Ref. 2010/600724.

11 Not used.

12 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732 Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/23759.

13 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-793 Revision 0. Westinghouse Electric Company LLC. March 2011. TRIM Ref. 2011/192251.

14 *AP1000 Master Submission List*. UKP-GW-GLX-001 Revision 0. Westinghouse Electric Company LLC. April 2011. TRIM Ref. 2011/246930.

15 *Nuclear Safety Criteria for the Design of Stationary PWR plants.* ANSI N18.2. American National Standards Institute. August 1973.

16 *AP1000 European Design Control Document*. EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC. 2009. TRIM Ref. 2011/81804.

17 *Step 4 Fuel and Core Design Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-005, Revision 0. TRIM Ref. 2010/581526.

18 *Step 4 Fault Studies – Containment and Severe Accident Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-004b, Revision 0. TRIM Ref. 2010/581405.

19 *Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-003, Revision 0. TRIM Ref. 2010/581527.

20 *Success Criteria for PSA for AP1000*. GRS-V-HSE-WP11-14-14a-01. GRS. January 2011. TRIM Ref. 2011/109368.

21 *WP01: Reactor Physics of AP1000.* GRS-V-HSE-WP01-01 Final Report. February 2011. Technical Support Services to the ND of HSE. GRS. TRIM Ref. 2011/369846.

22 *Develop an ATHLET Input Deck for AP1000*. GRS-V-HSE-WP3.2 & 3.4-01. GRS. January 2011. TRIM Ref. 2011/123312.

23 *Benchmark Analyses against WEC Analyses for a small break LOCA and the LONF as initiator for an ATWS.* GRS-V-HSE-WP3.3-01. GRS. March 2011. TRIM Ref. 2011/204655.

24 *GRS Technical Support Services to the ND of HSE. WP6: ATWS Analysis for UK AP1000.* GRS-V-HSE-WP06-01. GRS. February 2011. TRIM Ref. 2011/329042.

25 *WP18 and WP18a: Cooldown Fault Analysis for AP1000.* GRS-V-HSE-WP18/18a-02. GRS. March 2011. TRIM Ref. 2011/329033.

26 *WP5/5a: Technical Review of AP1000 Passive Core and Containment Cooling* Systems. GRS-V-HSE-WP05/5a-01. GRS. February 2011. TRIM Ref. 2011/201334.

27 *WP5b: Technical Review of AP1000 Passive Core and Containment Cooling Systems*, GRS-V-HSE-WP5b-01. GRS. July 2011. TRIM Ref. 2011/352699.

28 *Nuclear Safety Criteria for the Design of Stationary PWR plants. ANSI/ANS-51.1-1983.* American National Standards Institute (ANSI). 1983.

29 *Full Response to Regulatory Observation RO-AP1000-47, Diversity of Frequent Faults and Consideration of Passive Failures (Fault Studies).* Unique Number REG WEC 00479. Letter from AP1000 Project Front Office to ND. 18 January 2011. TRIM Ref. 2011/38780.

30 *Single Failure Criterion.* SECY-77-439. US NRC. August 1977.

31 *Sizewell B Station Safety Report, Chapter 15*. Nuclear Electric. 1992. HSE Library Reference: ID507708-1001.

32 *Response to Regulatory Observation RO-AP1000-47 Actions RO-AP1000-47.A2.1, A2.2 and A2.3.* Letter from AP1000 Project Front Office to ND. Unique Number REG WC 000458. 23 December 2010. TRIM Ref. 2010/643740.

33 *AP1000 UK Safety Categorisation and Classification of Systems, Structures and Components.* UKP-GW-GL-144 Revision 1. Westinghouse Electric Company LLC. January 2011. TRIM Ref. 2011/82081.

34 *AP1000 UK Safety Categorisation and Classification Methodology.* UKP-GW-GL-044 Revision 1. Westinghouse Electric Company LLC. April 2010. TRIM Ref. 2011/173949.

35 *Revised Response to RO-AP1000-052 Action A1.1 – Demonstration of Safe Shutdown.* Unique Number WEC 000524. Letter from AP1000 Project Front Office to ND. 28 February 2011. TRIM Ref. 2011/124352.

36 *UK AP1000 Probabilistic Risk Assessment.* UKP-G W-GL-022 Revision 0. Westinghouse Electric Company LLC. September 2008. TRIM Ref. 2010/401045.

37 *Response to RO-AP1000-46 and RO-AP1000-46.A1.1 – List of Design Basis Initiating Events Following ND Comments on the WEC Response of 28 May 2010.* Unique Number REG WEC 000290. Letter from AP1000 Project Front Office to ND. 10 August 2010. TRIM Ref. 2010/351527.

38 *Review of UK AP1000 PRA – Internal Initiating Events during Full Power Operation.* JEL-HSE-0309 Revision 2. Jacobsen Engineering Limited. April 2010. TRIM Ref. 2011/284471.

39 *A preliminary report of further secondary side blow down sensitivity studies for the Sizewell B PWR*. PWR/R 772. NNC Ltd. October 1983. HSE Library ID: 23558-1001

40 *Reactor Core Response to Excessive Secondary Steam Releases*. WCAP-9226-R1. Westinghouse Electric Company LLC. January 1978. TRIM Ref. 2010/441711.

41 *AP1000 HZP Steamline Break Analysis for SAR.* APP-SSAR-GSC-549 Revision 0. Westinghouse Electric Company LLC. November 2003. TRIM Ref. 2011/540660.

42 *AP600 LOFTRAN-AP and LOFFTR2 Final Verification and Validation report.* WCAP-14307 Revision 1. Westinghouse Electric Corporation LLC. August 1997. TRIM Ref. 2011/82138.

43 *VIPRE-01 Modelling and Qualification for Pressurised Water Reactor Non-LOCA Thermal Hydraulic Safety Analysis.* WCAP-14565-P-A. Westinghouse Electric Company LLC. October 1999. TRIM Ref. 2011/106554.

44 *FACTRAN: A FORTRAN IV Code for Thermal Transients in UO2 Fuel Rod*. WCAP-7908-A. Westinghouse Electric Company LLC. December 1989. TRIM Ref. 2011/535295.

45 *Sub-channel thermal-hydraulic analysis at AP600 low-flow steam line break conditions.* Nuclear Technology Volume 112. December 1995.

46 *Transient Analysis to Support the Generic Safety Case for Sizewell B.* C5166/TR/137. NNC. July 1998. HSE Library Reference: ID381891-1001.

47 *Evaluation of ATWS Events for the UK AP1000 Pressurised Water Reactor.* UKP-GW-GLR-016 Revision B. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/82101.

48 *Addition of Reactor Trip to Mitigate the Inadvertent PRHR Transient*. DCP APP-GW-GEE-1258 Revision 0. Westinghouse Electric Company LLC. March 2010. TRIM Ref. 2011/76305.

49 *LOFTRAN & LOFTTR2 AP600 Code Applicability Document*. SSAR-GSC-129 Revision 1: WCAP-14234 Revision 1. August 1997. TRIM Ref. 2011/535312 and WCAP-14235 Revision 1. September 1997. TRIM Ref. 2011/540697. Westinghouse Electric Company LLC.

50 *Response to RO-AP1000-48 and Action RO-AP1000-48.A1.1 Radiological Consequences*. Letter from AP1000 Project Front Office to ND. Unique Number WEC000400N. 29 October 2010. TRIM Ref. 2010/543558.

51 *Report of the Consequences of a postulated Main Feedline Rupture.* WCAP-9230. Westinghouse Electric Company LLC. January 1978. TRIM Ref. 2011/93276.

52 *AP1000 Code Applicability Report*. WCAP-15644-P Revision 2. Westinghouse Electric Company LLC. March 2004. TRIM Ref. 2011/102547.

53 *AP1000 PIRT and Scaling Assessment Report*. WCAP-15613 Revision 0. APP-GW-GL-502. Westinghouse Electric Company LLC. March 2001. TRIM Ref. 2011/93257.

54 *AP600 Design Certification Program SPES-2 Tests Final Data Report.* WCAP-14309 Revision 1. Westinghouse Electric Company LLC. July 1995. TRIM Ref. 2011/79981.

55 *AP600 SPES-2 Test Analysis Report*. PXS-T2R-11 Volume 1 and Volume 2. Revision 1. Westinghouse Electric Corporation. May 1995. TRIM Refs 2011/542975 and 2011/542986.

56 *Similarity analysis and scaling criteria for LWR's under single-phase and two-phase natural circulation.* NUREG/CR-3267. ANL-83-32. March 1983.

57 *Scaling analysis for the OSU AP600 test facility (APEX).* Nuclear Engineering and Design 186. pp 53-109. February 1998.

58 *AP600 Passive Residual Heat Removal Heat Exchanger Test Final Report.* WCAP-12980 Revision 3. Westinghouse Electric Company LLC. April 1997. TRIM Ref. 2011/79952.

59 *Scaling Analysis for AP600 Containment Pressure During Design Basis Accidents*. WCAP-14845 Revision 3. Westinghouse Electric Company LLC. March 1998. TRIM Ref. 2011/82150.

60 *Experimental Basis for the AP600 Containment Vessel Heat and Mass Transfer Correlations.* WCAP-14326 Revision 3. Westinghouse Electric Company LLC. April 1998. TRIM Ref. 2011/93239.

61 *AP1000 Steam Generator Tube Rupture Margin to Overfill Analysis to Investigate the Impact of Containment Back Pressure*. APP-SSAR-GSC-736 Revision 0. Westinghouse Electric Company LLC. August 2009. TRIM Ref. 2011/81679.

62 *FWS/CVS isolation on SGS High Alarm*. DCP APP-GW-GEE-1294 Revision 6. Westinghouse Electric Company LLC. February 2010. TRIM Ref. 2011/76317.

63 *AP1000 Anticipated Transient without SCRAM analysis using LOFTRAN code.* APP-GL-GSC-012 Revision 0. Westinghouse Electric Company LLC. May 2002. TRIM Ref. 2011/540610.

64 *AP1000 Anticipated Transient without SCRAM sensitivity study.* APP-GL-GSC-009 Revision 0. Westinghouse Electric Company LLC. March 2002, updated March 2003. TRIM Ref. 2011/540600.

65 *AP1000 Additional Information Related to ATWS events.* APP-SSAR-GSC-634. Westinghouse Electric Company LLC. February 2004. TRIM Ref. 2011/540643.

66 *Loss of Normal Feedwater Event with Diverse Mitigation.* UKP-SSAR-GSC-009. Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/93204.

67 *AP1000 Design Transients: Loss of Offsite Power.* APP-RCS-M1C-018 Revision 0. Westinghouse Electric Company LLC. October 2004. TRIM Ref. 2011/540625.

68 *AP1000 Plant Parameters*. APP-GW-G0-002 Revision 2. Westinghouse Electric Company LLC. November 2003. TRIM Ref. 2011/93478.

69 *IRWST Heatup with FPL Wet Bulb Temperature.* APP-PXS-M3C-060 Revision 0. Westinghouse Electric Company LLC. June 2009. TRIM Ref. 2011/137900.

70 *AP1000 RNS Plant Cooldown Performance Calculation.* APP-RNS-M3C-003 Revision 3. Westinghouse Electric Company LLC. March 2010. TRIM Ref. 2011/137905.

71 *AP600 Low Flow Critical Heat Flux (CHF) Test Data Analysis.* WCAP-11397-P-A Revision 0. Westinghouse Electric Company LLC. May 1995. TRIM Ref. 2011/79984.

72 *Revised Thermal Design Procedure.* WCAP-14371-P-A. Westinghouse Electric Company LLC. April 1989. TRIM Ref. 2011/106728.

73 *Westinghouse Response to RO-AP1000-050 Action A1.1, Demonstration of Protection against PCI Failure.* Unique Number WEC 000365. Westinghouse Electric Company LLC. September 2010. TRIM Ref. 2010/493368.

74 *Full Response to Regulatory Observation RO-AP1000-91. Use of Incore Detectors to Protect against Adverse Power Distributions*. Letter from AP1000 Project Front Office to ND. Unique Number WEC 000502. 7 February 2011. TRIM Ref. 2011/78351.

75 *Implementation of P-17 for Rod Withdrawal Prohibit*. DCP APP-GW-GEE-1304 Revision 0. Westinghouse Electric Company LLC. February 2010. TRIM Ref. 2011/76320.

76 *Refuelling Error on Dampierre Unit-4.* IRS number 7505. International Incident Reporting System (IRS). IAEA. April 2001.

77 *An evaluation of the rod ejection accident in Westinghouse Pressurised Water Reactors using spatial kinetics methods.* WCAP-7588 Revision 1-A. January 1975. Westinghouse Electric Company LLC. TRIM Ref. 2011/535608.

78 *Sizewell B RCCA ejection analysis at Hot Full Power End of Cycle conditions.* PWR/R 991. NNC Ltd. March 1987. HSE Library Reference: ID20721-1001.

79 *RIA Fault Study Margin.* Revised analysis submitted under cover of *Westinghouse Response to RO-AP1000-063 Action A1.1*. Unique Number REG WEC 000364. Westinghouse Electric Company LLC. Sept 2010. TRIM Ref. 2011/93515.

80 *AP1000 Steam Generator Tube Rupture Analysis.* APP-SSAR-GSC-516 Revision 0. CN-CRA-01-93. Westinghouse Electric Company LLC. May 2002. TRIM Ref. 2011/540639.

81 *TRACE analysis of a Steam Generator Tube Rupture Event for the AP1000.* 15972/TR/002 Issue 2. AMEC. February 2011. TRIM Ref. 2011/112772.

82 APP-SSAR-GSC-516 Revision 0 (provided in Response to TQ-AP1000-202). Westinghouse Electric Company LLC. TRIM Ref. 2011/542969.

83 *AP1000 Steam Generator Tube Rupture Analysis for the Advanced First Core*. APP-SSAR-GSC-174 Revision 0. Westinghouse Electric Company LLC. November 2009. TRIM Ref. 2011/81655.

84 *R.N. Lewis et al*. *SGTR Analysis Methodology to Determine the Margin to Steam Generator Overfill*. WCAP-10698-P-A (Proprietary). August 1987. TRIM Ref. 2011/535298, WCAP-10750-A (Non Proprietary). March 1987. TRIM Ref. 2011/540683.

85 *Review of the LOFTRAN passive systems code models and analysis with respect to the HSE Safety Assessment Principles FA17 to FA24 in support of the UK GDA for the Westinghouse AP1000 reactor system.* AMEC report 15972/TR/0001 Issue 02. May 2010. TRIM Ref. 2010/218241.

86 *ND BMS. Validation of Computer Codes and Calculational Methods.* T/AST/042 Issue 1. HSE. July 2000. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast042.pdf.

87 *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design* (NUREG-1793). September 2004. www.nrc.gov/reading-rm/doc/collections/nuregs/staff/sr1793/.

88 *AP1000 RCS Depressurization Analyses for DCD.* APP-SSAR-GSC-541 Revision 0. (Supplied with TQ-AP1000-333). Westinghouse Electric Company LLC. TRIM Ref. 2011/540641.

89 *TRACE Analysis of a 10 inch Cold Leg Break Loss of Coolant Event for the AP1000.* 16423/TR/0001 Issue 02. AMEC. November 2010. TRIM Ref. 2010/609749.

90 *NOTRUMP Final Validation Report for AP600.* WCAP-14807 Volumes 1, 2 and 3. Revision 5. Westinghouse Electric Company LLC. August 1998. TRIM Refs 2011/540715, 2011/540722 and 2011/540735.

91 *CMT sizing/performance for AP1000.* APP-PXS-M3C-004 Revision 0. Westinghouse Electric Company LLC. May 2002. TRIM Ref. 2011/94171.

92 *Accumulator Sizing/performance for AP1000.* APP-PXS-M3C-005 Revision 0. February 2002. Westinghouse Electric Company LLC. TRIM Ref. 2011/542696.

93 Low pressure integral systems test at Oregon State University. Final Data Report. Volume 1 – 4. WCAP-14252. September 1998. TRIM Refs 2011/79972, 2011/79973, 2011/79976 and 2011/79977.

94 *APEX-AP1000 Confirmatory Testing to Support AP1000 Design Certification (Proprietary).* NUREG-1826. US NRC. June 2005.

95 *Core Make-up Tank Test Data Report.* WCAP-14217. Westinghouse Electric Corporation. November 1994. TRIM Ref. 2011/79970.

96 *Non Condensable gas effects in ROSA/AP600 Small-Break LOCA experiments.* International Conference on Nuclear Engineering Volume 1 – Part A. ASME 1996.

97 *Core Make-Up Tank Behaviour Observed during the ROSA-AP600 experiments.* Nuclear Technology Volume 119. August 1997.

98 *UK/NII DEDVI Line Break with Failed Accumulator Check Valve or Failed CMT Check Valve.* UKP-SSAR-GSC-006 Revision 0. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/82131.

99 *Double-Ended DVI with Failure of Intact CMT.* OSU-APEX-97014 Revision 0. (NRC-28). APEX Long-term Cooling Test Facility. Oregon State University. November 1997.

100 *Double-Ended DVI with Failure of Intact Acc.* OSU-APEX-97015 Revision 0. (NRC-29). APEX Long-term Cooling Test Facility. Oregon State University. November 1997.

101 *SBLOCA Event with Bounding Assumptions to Demonstrate Diversity (I and II).* UKP-SSAR-GSC-010 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/93206.

102 *AP1000 Best Estimate Large Break LOCA (BELOCA) Response to UK NII TQ-AP1000-673: LBLOCA with Accumulator Check Valve Failure*. LTR-LIS-10-630 Revision 0. October 2010. TRIM Ref. 2010/558598.

103 *Code Qualification Document for Best Estimate Loss of Coolant Accident Analysis*. WCAP-12945-P-A Revision 2. Westinghouse Electric Company LLC. March 1998. TRIM Refs 2010/320857, 2010/321051, 2010/321119.

104 *WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-coolant Accident.* WCAP-14171 Revision 2. Westinghouse Electric Company LLC. March 1998. TRIM Ref. 2011/102491.

105 NUREG/CR-5249, Rev. No. 4, "Quantifying Reactor Safety Margins Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large-Break, LOCA." Accession Number: ML030380503. Date Released: Thursday, February 20, 2003.

106 *A Comparative Assessment of Clad Ballooning for the AP1000 PWR*. E.004067.03.07/01 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/99354.

107 *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design Docket No 52-006*. Chapter 4. NUREG-1793. September 2004.

108 *Realistic Large-Break LOCA Evaluation Methodology Using the Automated Statistical Treatment of Uncertainty Method (ASTRUM)*. WCAP-16009-P Revision 0. Westinghouse Electric Company LLC. May 2003. TRIM Ref. 2011/102524.

109 *MATARE Clad Ballooning Assessment of the AP1000 LBLOCA Transient*. C16507/TR/0001 Issue 1. AMEC. February 2011. TRIM Ref. 2011/102623.

110 *Safety Significance of the Halden IFA-650 LOCA Test Results*. NEA/CSNI/R(2010) Issue 5. Organisation for Economic Co-operation and Development. November 2010. TRIM Ref. 2011/102575.

111 *AP1000 Spurious PMS events for UK.* October 2010. TRIM Ref. 2011/93775. Submitted under cover of Westinghouse Letter UN WEC0392N. 15 October 2010. TRIM Ref. 2010/524107.

112 *AP1000 Shutdown and Spent Fuel Pool Faults.* UKP-GW-GL-077 Revision 0. Westinghouse Electric Company LLC. January 2011. TRIM Ref. 2011/82078.

113 *AP1000 Implementation of the Regulatory Treatment of Nonsafety Related System Process.* WCAP-15985 Revision 2. August 2003. TRIM Ref. 2011/535341. Provided in response to TQ-AP1000-310.

114 *Step 4 Radiological Protection Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-009 Revision 0. TRIM Ref. 2010/581522.

115 *Step 4 Civil Engineering and External Hazards Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-002, Revision 0. TRIM Ref. 2010/581528.

116 *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States.* NUREG-1449. US Nuclear Regulatory Commission. September 1993.

117 *Step 4 Internal Hazards Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-001, Revision 0. TRIM Ref. 2010/579786.

118 *AP1000 Internal Hazards Topic Report*. UKP-GW-GLR-001 Revision 2. Westinghouse Electric Company LLC. September 2010. TRIM Ref. 2011/82084.

119 *AP1000 Main Steamline Break Doses to Support Regulatory Observation 48*. UKP-SSAR-GSC-008. Westinghouse Electric Company LLC. January 2011. TRIM Ref. 2011/82132.

120 *LOFTRAN Code Description.* WCAP-7907-P-A. Westinghouse Electric Corporation LLC. April 1984. TRIM Ref. 2011/535286.

121 *Radiological Analysis – Fault Conditions.* T/AST/045 Issue 01. HSE. 10 June 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast045.htm

122 *AP1000 DBA Radiological Consequences Assessments*. 15972/TR/0003 Issue 2. AMEC. January 2011. TRIM Ref. 2011/57129.

123 *Realistic methods for calculating the release of radioactivity following steam generator tube rupture faults*. *A consensus document*. EUR 15615 EN. December 1994. ISBN-10: 9282686671. ISBN-13: 978-9282686676.

124 *Determination of the in-containment source term for a Large Break Loss of Coolant Accident.* EUR 19841 EN. April 2001.

125 *1990 Recommendations of the International Commission on Radiological Protection*. Annals of the ICRP Volume 21 No.1-3. ICRP Publication 60. ICRP. September 1992. Elsevier. ISBN 10**:** 0-08-041998-4. ISBN 13: 978-0-08-041998-5.

126 *Full Response to RO-AP1000-94 Actions A1 to A5, GDA Design Basis Limits and Development of Plant Operating Limits.* Westinghouse Electric Company LLC. Unique REG WEC 000446. December 2010. TRIM Ref. 2010/622558.

127 *Reactor Coolant Design Transients.* APP-RCS-M1-001 Revision 2. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/81641.

128 *Step 4 Structural Integrity Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-011, Revision 0. TRIM Ref. 2010/581520.

129 *New Nuclear Power Stations Generic Design Assessment – Safety assessment in an international context*. Version 3, HSE. March 2009. www.hse.gov.uk/newreactors/ngn05.pdf.

130 *New Nuclear Power Stations Generic Design Assessment – Strategy for working with overseas regulators*. HSE. March 2009. www.hse.gov.uk/newreactors/ngn04.pdf.

131 *Step 4 Reactor Chemistry Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-008, Revision 0. TRIM Ref. 2010/581523.

132 *SPWR Passive Residual Heat Removal Heat Exchanger performance for LOCA and Non-LOCA events.* 7th International Conference on Nuclear Engineering, Tokyo, Japan. ICONE-7221. April 19-23, 1999.

133 *Step 4 Mechanical Engineering Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-010, Revision 0. TRIM Ref. 2010/581521.

134 *Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-007, Revision 0. TRIM Ref. 2010/ 581525.

135 *GDA Issue GI-AP1000-FS-01 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80890.

136 *GDA Issue GI-AP1000-FS-02 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80898.

137 *GDA Issue GI-AP1000-FS-03 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80905.

138 *GDA Issue GI-AP1000-FS-04 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80913.

139 *GDA Issue GI-AP1000-FS-05 Revision 1. Background and explanatory information.* TRIM Ref. 2011/80921.

140 *GDA Issue GI-AP1000-FS-06 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80929.

141 *GDA Issue GI-AP1000-FS-07 Revision 0. Background and explanatory information.* TRIM Ref. 2011/80936.

142 *GDA Issue GI-AP1000-FS-08 Revision 0. Background and explanatory information.* TRIM Ref. 2011/289580.

143 *Westinghouse Reload Safety Evaluation Methodology.* WCAP-9272-P-A. July 1985. TRIM Ref. 2011/535625.

144 *Step 4 Cross-cutting Topics of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-032, Revision 0. TRIM Ref. 2010/581499.

145 A Review of the Sizewell B Pre-Operational Safety Report Chapter 15, Sections 5, 6 and 7 – Design Basis Fault Analysis. AR B5/PWR/02/94. Issue 2. NUC 552/74/01. HSE. December 1994. TRIM Ref. 2011/574615.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-01	The future licensee shall review the Categorisation and Classification methodology report (UKP-GW-GL-044, Rev 1) for consistency with the requirements of the response to RO-AP1000-47 (UKP-GW-GL-067, Rev 0).	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-02	The future licensee shall review the Categorisation and Classification report to ensure consistency for the PLS between requirements in the response to RO-AP1000-47 (Report UKP-GW-GL-067, Rev 0) which requires Class A2 and the assignment in the Categorisation and Classification report (UKP-GW-CL-144, Rev 1) which proposes Class B2.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-03	The future licensee shall review the Classification of the manual actuations on the PLS for consistency with the claims in the response to RO-AP1000-47 (UKP-GW-GL-067, Rev 0), which require Class A2 standard.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-04	The future licensee shall justify the adequacy of the safe shutdown state condition defined in the response to RO-AP1000-52 (UKP-GW-GL-079, Rev 1).	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-05	The future licensee shall provide a design basis safety case for interfacing LOCAs or demonstrate that they are beyond the design basis.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-06	The future licensee shall review the findings from the response to AF-AP1000-PSA-13 to see if there are any additional initiating events that need to be considered as new design basis faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-07	The future licensee shall review the core design assumed in the design basis safety analysis for main steamline break fault for consistency with the AP1000 core design.	Fuel on-site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-08	The future licensee shall demonstrate that the fault analysis of the main steamline break fault from hot zero power is conservative or perform analysis using a coupled code.	Fuel on-site
AF-AP1000-FS-09	The future licensee shall review the validation evidence applied by Westinghouse to the modelling of buoyancy dominated flow conditions in the main steamline break analysis to confirm that it is adequate for the purpose.	Fuel on-site
AF-AP1000-FS-10	The future licensee shall provide justification for the use of the W-3 CHF correlation for the low pressures, flows and high qualities associated with a main steamline break fault at hot zero power conditions.	Fuel on-site
AF-AP1000-FS-11	The future licensee shall perform an assessment of the effect of a main steamline break at hot zero power for the conditions of zero xenon and zero boron but without a stuck RCCA.	Fuel on-site
AF-AP1000-FS-12	The future licensee shall demonstrate that for the stuck open SG relief or safety valve fault with common mode failure of the RCPs to trip, the relevant acceptance criteria are met to ensure the position is ALARP.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-13	The future licensee shall demonstrate that the MFW pump trip provides adequate diversity for feedline isolation for a stuck open relief or safety valve fault at hot zero power, or alternatively demonstrate the acceptability of the consequences of this function failing.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-14	The future licensee shall demonstrate that the closure of the turbine stop valves provides adequate diversity of steamline isolation for the excessive increases in secondary side steam flows, or alternatively demonstrate the acceptability of the consequences of this function failing.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-15	The future licensee shall provide analysis of the stuck open relief or safety valve fault for hot zero power conditions assuming two stuck RCCAs to demonstrate that such an event is less limiting than the MSLB fault with failure of one RCCA to insert.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-16	The future licensee shall develop a safety case covering the transition from controlled state to safe shutdown state for increase in heat removal faults, decrease in heat removal faults and reactivity and adverse power distribution faults. Fault-specific operator actions should be clearly identified.	Fuel on-site
AF-AP1000-FS-17	The future licensee shall demonstrate that bleed and feed provides a diverse means of protecting against the feedline break fault following the passive single failure of the PRHR isolation valve.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-18	The future licensee shall analyse the results of the natural circulation test and the PRHR test performed on the first of a kind AP1000 plant during power ascension to confirm that the performance of the PRHR is consistent with the claims made in safety case. Alternatively, the licensee shall perform these tests on its first plant built in the UK.	Fuel on-site. Alternatively, Power raise if test is performed in the UK.
AF-AP1000-FS-19	The future licensee shall analyse the results of the PRHR test and the IRWST heat-up tests during the pre-operational hot functional tests performed on the first of a kind AP1000 plant to confirm that the performance of the PRHR and the IRWST are consistent with the claims made in safety case. Alternatively, the licensee shall perform these tests on its first plant built in the UK.	Fuel on-site. Alternatively, Fuel Load if the test is performed in the UK.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-20	The future licensee shall provide details of the analysis performed to justify the adequacy of the sizing of the pressuriser to protect against RCS overpressurisation for the inadvertent MSIV closure fault with common mode failure of the PSVs such that appropriately justified acceptance criteria are met.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-21	The future licensee shall provide transient analysis to justify the adequacy of the SG PORVs to provide diverse protection against SG overpressure following the inadvertent MSIV closure fault with common mode failure of the MSSVs such that appropriately justified acceptance criteria are met.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-22	The future licensee shall provide transient analysis to demonstrate the effectiveness of the DAS to provide diverse protection against the loss of normal feedwater fault with common mode failure of the PMS such that appropriately justified acceptance criteria are met.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-23	The future licensee shall provide transient analysis for the loss of normal feedwater fault (and the additional failure of the start-up feedwater system) with common mode failure of the PRHR to demonstrate that significant fuel damage can be prevented by the CMTs automatically actuating the ADS. Alternatively, it shall identify the maximum timescales available for manual actuation of bleed and feed to avoid significant fuel damage and justify that these are adequate.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-24	The future licensee shall provide validation evidence on the applicability of the RELAP-5 computer code for performing safety analyses for the frequent fault diversity analysis of the AP1000 design. Alternatively, verified computer codes used in the analysis of AP1000 design basis events should be used to replace the RELAP-5 safety analysis.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-25	The future licensee shall provide transient analysis to demonstrate the ability of the start-up feedwater pumps to prevent PSV lifting following the loss of normal feedwater fault using appropriately conservative analysis consistent with the sequence frequency.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-26	The future licensee shall revise the response to RO-AP1000-52 to remove the incorrect reference to HSE-ND having confirmed the performance of the PCS.	Nuclear Island Safety Related Concrete
AF-AP1000-FS-27	The future licensee shall confirm that the sizings of the RNS, CCS, & SWS systems are sufficient to provide a diverse ultimate heat sink function to cool the IRWST following the loss of normal feedwater fault (including loss of SFW) and a SBLOCA fault following common mode failure of the PCS against Condition IV acceptance criteria and appropriately conservative analysis consistent with the sequence frequency subject to ALARP.	Nuclear Island Safety Related Concrete
AF-AP1000-FS-28	The future licensee shall provide a safety case including design basis transient analysis to demonstrate adequate protection against RCS overpressure following the loss of normal feedwater fault (including loss of SFW) with common mode failure of the PSVs.	Nuclear Island Safety Related Concrete
AF-AP1000-FS-29	The future licensee shall perform as part of the commissioning test programme a load follow demonstration of the AP1000 or alternatively provide justification of why the testing on other AP1000 units remains applicable for the UK recognising that the turbine control systems for any UK plant are likely to be UK specific.	Following Sync to grid
AF-AP1000-FS-30	The future licensee shall demonstrate that diverse protection exists for the uncontrolled RCCA bank withdrawal fault for the full range of rod speeds and power levels using appropriately conservative analysis assumptions and acceptance critieria subject to ALARP.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-31	The future licensee shall demonstrate that the uncontrolled RCCA bank withdrawal fault with failure of RCCAs to insert ATWT case is bounded by the failure of PMS to trip ATWT case.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-32	The future licensee shall develop proposals for demonstrating the adequate performance of the in-core detectors on the first of kind AP1000 plant in the UK.	Power raise
AF-AP1000-FS-33	The future licensee shall demonstrate that for the frequent SGTR fault there is a diverse means of protection for each safety function or that the radiological consequences are ALARP and meet the requirements of Target 4 of the SAPs in reaching the controlled state.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-34	The future licensee shall analyse the spectrum of SGTR faults with a size greater than make-up capacity of the CVS (<2A) up to multiple tube ruptures all in the same SG and demonstrate that the 2A tube rupture is bounding.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-35	The future licensee shall justify what fault sequences and SCCs they are claiming for the frequent SGTR fault and demonstrate how all safety criteria are met in reaching the safe shutdown state.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-36	The future licensee shall analyse the results of the ADS blow down tests to confirm the performance of the ADS, spargers and CMTs during the pre-operational hot functional tests performed on the first of a kind reactor. Alternatively, the licensee shall perform these tests on its first plant built in the UK.	Fuel on-site Alternatively, Fuel load if the tests are performed in the UK.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-37	The future licensee shall analyse the results of the CMT recirculation tests to confirm the performance of the CMT system meets the requirements of the safety case during the pre-operational hot functional tests performed on the first of a kind reactor. Alternatively, the licensee shall perform these tests on its first plant built in the UK.	Fuel on-site Alternatively, Fuel Load if the test is performed in the UK.
AF-AP1000-FS-38	The future licensee shall demonstrate that the thermal hydraulic interactions between the spargers cannot threaten the structural integrity of the IRWST tank and injection lines.	Nuclear Island Safety Related Concrete
AF-AP1000-FS-39	The future licensee shall demonstrate that the fault analysis reported in the EDCD for the DVI line break fault with the single failure of an ADS-4 valve provides adequate margin. Alternatively a coupled containment and RCS thermal hydraulic analysis may be provided.	Fuel on-site.
AF-AP1000-FS-40	The future licensee shall verify that testing exists to address the important phenomena identified in the PIRT for DVI line break fault with the single failure of the CMT check valve on the intact DVI line is satisfied by the testing performed for the AP1000. Alternatively a scaled integral test (possibly on the APEX facility) may be performed to confirm that the predictions in the safety analysis are valid. HSE-NDs strong preference is for testing to be performed.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-41	The future licensee shall verify that testing exists to address the important phenomena identified in the PIRT for DVI line break fault with the single failure of the accumulator check valve on the intact DVI line is satisfied by the testing performed for the AP1000. Alternatively a scaled integral test (possibly on the APEX facility) may be performed to confirm that the predictions in the safety analysis are valid. HSE-NDs strong preference is for testing to be performed.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-42	The future licensee shall perform transient analysis to demonstrate adequate protection against the frequent SBLOCA fault with failure of the RCCAs to insert.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-43	The future licensee shall demonstrate the structural integrity of the ADS Stage-4 lines following actuation of ADS Stage-4 valves during a frequent fault SBLOCA in which there is creditable common mode failure of the ADS Stages 1-3 valves to open. PRHR operation may be assumed.	Nuclear Island Safety Related Concrete
AF-AP1000-FS-44	The future licensee shall perform transient analysis to demonstrate adequate protection against the frequent SBLOCA fault with common mode failure of the containment isolation valves and that the radiological releases are ALARP and meet the requirements of SAP Target 4.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-45	The future licensee shall demonstrate that the pressuriser low-pressure trip provides adequate protection against DNB following a spurious operation of either an ADS Stage-1 valve or a PSV valve.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-46	The future licensee shall provide site specific design basis radiological consequences analysis, taking due cognisance of UK methodology assumptions and explicitly comparing against SAP Target 4. Assumptions and limits need to be justified and applied consistently to allow judgements to be made on whether the risks are ALARP. Limiting single failures in both the radiological consequences analysis and the accompanying thermal hydraulic analysis need to be reviewed to check that assumptions across the two are consistent and limiting.	Fuel on-site
AF-AP1000-FS-47	The future licensee shall ensure that future fuel reloads are consistent with the assumptions made in the safety analysis for the LBLOCA fault with failure of one accumulator.	Fuel on-site

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-FS-48	The future licensee shall propose a suitable surveillance procedure to confirm that the axial power distribution has not deviated from the assumptions of the safety case.	Fuel on-site
AF-AP1000-FS-49	The future licensee shall perform an assessment of the spurious pressuriser spray with failure of PMS to trip ATWT case to demonstrate that the appropriate acceptance criteria are met subject to ALARP.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-50	The future licensee shall provide a safety case to demonstrate adequate protection against spurious operation of the PLS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-51	The future licensee shall provide a safety case to demonstrate adequate protection against spurious operation of the PMS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site
AF-AP1000-FS-52	The future licensee shall provide a safety case to demonstrate adequate protection against spurious operation of the DAS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – before delivery to Site

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the Regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Fault Studies – Design Basis Faults – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SPENT FUEL POOL SAFETY CASE

GI-AP1000-FS-01 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Electrical Engineering Mechanical Engineering Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-01**	**GDA Issue Action Reference**	**GI-AP1000-FS-01.A1**
GDA Issue	The design basis case developed in GDA Step 4 for the spent fuel pool for the Fault Studies topic area needs to be cascaded into other technical areas and any new claims clearly identified in the PCSR. The design change process needs to be followed to incorporate the various physical modifications identified and all the affected documents need to be updated. Fault Studies concerns on the availability of the RNS and the protection of fuel above the spent fuel racks are to be addressed.		
GDA Issue Action	Westinghouse to identify the impact of the new spent fuel pool safety case on relevant sections of the PCSR and report / discuss the implications with the relevant ONR topic leads in an appropriate manner. It is likely that Westinghouse will need to provide supplementary information to allow ONR to consider in detail the specifics of the design changes and the capability of SSCs to deliver newly identified safety functions. Westinghouse to revise the PCSR and other affected documents to reflect the updated safety case and all new safety claims. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SPENT FUEL POOL SAFETY CASE
GI-AP1000-FS-01 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Electrical Engineering Mechanical Engineering Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-01**	**GDA Issue Action Reference**	**GI-AP1000-FS-01.A2**
GDA Issue Action	Westinghouse to complete the design change process for the identified modifications to the spent fuel pool active cooling system and blow out panels. The proposed design changes are to provide an engineered connection from the fire fighting system to supply cooling water to the CCW heat exchanger and to add filters to the ventilation blowout panels on the spent fuel pool. These modifications will limit the frequency of pool boiling to less than 10^{-3} per year and meet ONR's expectations on ventilation and preservation of barriers set out in SAPs ECV.1, ECV.2 and FA.7. These design changes need to be complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SPENT FUEL POOL SAFETY CASE

GI-AP1000-FS-01 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Electrical Engineering Mechanical Engineering Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-01**	**GDA Issue Action Reference**	**GI-AP1000-FS-01.A3**
GDA Issue Action	Westinghouse to update the relevant parts of the safety case to address outstanding concerns on the consequences of a fault occurring while fuel is being moved above the racks, and on competing claims in the availability of the RNS. The safety case provided for the Spent Fuel Pool does not adequately address the consequences of faults occurring while fuel is being moved above the racks. It is also not clear if it is planned for the RNS to be available without restriction for spent fuel pool cooling in response to operational requirements, or if its use will be subject to time constraints defined by Technical Specification. This has relevance for the GDA Issue on the RNS design for RCS safety injection following a LOCA (GI-AP1000-FS5). No safety claims were made on the function of the RNS in the EDCD other than for its piping to retain its integrity. However, as a result of Step 4 Regulatory Observation responses, claims are now made in the UK safety case for both the reactor and the spent fuel pool. Further information is therefore required from Westinghouse to identify if competing claims are of concern. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN REFERENCE POINT AND ADEQUACY OF DESIGN BASIS ANALYSIS

GI-AP1000-FS-02 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-FS-02**	**GDA Issue Action Reference**	**GI-AP1000-FS-02.A1**
GDA Issue	Westinghouse to demonstrate for all design basis faults that the submitted design basis analysis is appropriate for the agreed GDA Design Reference Point and that all safety claims are supported by the analysis. If this cannot be done with pre-existing analysis, new analysis could be required. The final PCSR produced for GDA is to summarise this analysis for all design basis faults. A complete and consistent set of core design limits reflecting the design basis fault analysis is required.		
GDA Issue Action	Westinghouse to demonstrate that the transient analysis presented and/or referenced in the PCSR is appropriate for the agreed GDA Design Reference Point. Westinghouse to review the safety case and transient analysis presented in the PCSR for all design basis faults (including shutdown faults not part of the AFCAP programme) and for each: • identify to ONR what computer models, assumptions and reference design the EDCD analysis was assessed with and demonstrate why this is appropriate for the GDA Design Reference Point, or • replace the EDCD analysis with AFCAP analysis, identify what computer models, assumptions and reference design have been used for AFCAP, demonstrate the differences between the AFCAP work and the EDCD analysis ONR has assessed in Step 4, and demonstrate why this is appropriate for the GDA Design Reference Point, or • provide new analysis appropriate for the GDA Reference Point. The final GDA PCSR will need to clearly demonstrate why the analysis it references is appropriate for the Design Reference Point. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
DESIGN REFERENCE POINT AND ADEQUACY OF DESIGN BASIS ANALYSIS
GI-AP1000-FS-02 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-FS-02**	**GDA Issue Action Reference**	**GI-AP1000-FS-02.A2**
GDA Issue Action	Provide a complete set of core design limits reflecting the final design basis analysis in the PCSR and the Design Reference Point to determine the compliance of candidate core designs. Design basis analysis of reactor faults is generally carried out on a generic basis, with the intention that it will not need to be repeated for particular core loading patterns. The analysis assumes certain bounding core performance parameters (safety analysis bounding limits) that the core design is expected to respect. The core design assumed for in the EDCD design basis analysis is different from that assumed in the AFCAP work (in addition to all the other design changes to "fixed" systems). A part complete list has been provided to ONR in Step 4 of GDA in the form of a Safety Analysis Check List. However this does not reflect all the analysis presented in the PCSR (a mixture of EDCD and AFCAP work), Regulatory Observations and the Design Reference Point. For example, the Anticipated Transient Without Trip and Large Break Loss of Coolant Accident analyses are inconsistent with the check list. This set of data needs to be complete and comprehensive to determine a suitable set of constraints for core design. Should a future core design not respect these constraints, this could of course be justified by specific analysis or a new core design. However, without a clear link back to the analysis assessed in GDA, the goal of not repeating analysis for individual core loading patterns will be difficult to achieve. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Control and Instrumentation Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A1**
GDA Issue	Demonstration of functional diversity for frequent faults.		
GDA Issue Action	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. These should be referenced within the PCSR as the limits and conditions as the relevant core parameters identified by the fault studies for ultimate incorporation within the technical specifications for the AP1000 (see also GDA issue GI-AP1000-FS2). Alternatively, Westinghouse may wish to provide a revised analysis with parameters consistent with those presented in Chapter 4 of the DCD. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Control and Instrumentation Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A2**
GDA Issue Action	• 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. In the European DCD and the UKP-GW-GLR-016, the analysis of excessive increase in secondary steam flow with failure to trip is limited to consideration of the condition II event, which limits flow increases to less than 10% at full power. Westinghouse has not presented any analysis for a more challenging excessive increase in secondary steam flow fault at full power. Westinghouse will need to demonstrate adequate diverse protection for such faults for both the case with successful reactor trip and for 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. In particular, in the case of PMS failure, Westinghouse will have to demonstrate that there are adequate trip parameters on the diverse actuation system (DAS). Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Control and Instrumentation Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A3**
GDA Issue Action	• 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. The analysis of these faults presented by Westinghouse assumes that although the protection and monitoring system (PMS) is unavailable the flux monitoring system remains available to the plant control system (PLS) and provides protection against these faults. This fails to demonstrate any diversity within the flux protection system. For this reason, Westinghouse are requested to provide explicit transient analysis using design basis analysis techniques for these faults to demonstrate that the diverse actuation system (DAS) is functionally capable of protecting against this fault. A modification to include the provision of a negative rate flux trip signal on the diverse actuation system (DAS) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion with the PCSR. Note this action is also closely related to GDA issue GI-AP1000-FS.4. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Control and Instrumentation Probabilistic Safety Assessment	
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A4**
GDA Issue Action	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. Westinghouse has identified that a modification is required to provide a reactor trip signal on high hot leg temperature on the Diverse Actuation System. This is to protect against a RCCA bank withdrawal fault at full power with failure of the Protection and Monitoring System (PMS). The design for the proposed modification will need to complete the six-stage modification process for inclusion within the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Control and Instrumentation Probabilistic Safety Assessment	
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A5**
GDA Issue Action	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 either mechanical failure of the rods to insert or failure of the reactor protection system. In the Westinghouse submissions assessed, the analysis of complete loss of flow fault with failure to trip is limited to consideration of initial conditions associated with nominal full power conditions. Westinghouse has not presented any analysis considering the effect of grid perturbations on the initial reactor conditions. It is likely that in such circumstances, the reactor control system will attempt to increase power to compensate for any grid frequency reduction. This will perturb both the initial reactor power and the initial power distribution of the core including the axial offset. Westinghouse will need to demonstrate adequate diverse protection for such faults for both the case with successful reactor trip and for 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. In particular, in the case of PMS failure, Westinghouse will have to demonstrate that there are adequate trip parameters on the diverse actuation system (DAS). Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Control and Instrumentation Probabilistic Safety Assessment		
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A6**
GDA Issue Action	• 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 accident frequency targets. After every reactor trip from full power there is an eventual decay in the level of xenon poisoning within the reactor core. The resultant swing in reactivity needs to be compensated for through increasing the boron concentration in the reactor to ensure an adequate shutdown margin. While the core make-up tanks (CMTs) and the in-containment refuelling water storage tank (IRWST) systems provide two diverse sources of borated water should the operator fail to ensure adequate shutdown margin using the Chemical and Volume control system (CVS), both these systems are also dependent upon operator action for actuation. Although timescales are long (many hours), this implies a combined human reliability of 1×10^{-7} per demand to meet the design basis target. For this reason, Westinghouse is to provide an ALARP study into the feasibility of automatically actuating the CVS to inject borated water after every reactor trip and for the CMTs to be automatically actuated following failure of the CVS. Alternatively, Westinghouse may wish to provide a consequence analysis of what would happen should the operator fail to ensure adequate shutdown margin. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-AP1000-FS-03 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Control and Instrumentation Probabilistic Safety Assessment	
GDA Issue Reference	**GI-AP1000-FS-03**	**GDA Issue Action Reference**	**GI-AP1000-FS-03.A7**
GDA Issue Action	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. This fault would be very difficult to detect should there be a failure of the flux instrumentation or the protection and monitoring system (PMS). For this reason, Westinghouse is to provide explicit transient analysis using design basis analysis techniques for this fault to demonstrate that the diverse actuation system (DAS) is functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a boron dilution block signal and a CMT actuation signal on the DAS (actuated by low doubling time and/or high source-range flux level) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the PCSR. Westinghouse also needs to identify as a limit and condition for the reactor core design technical specifications the limiting moderator reactivity coefficients assumed in the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PROVISION OF ENHANCED AND DIVERSE FLUX PROTECTION TO PROTECT AGAINST ADVERSE POWER DISTRIBUTION FAULTS

GI-AP1000-FS-04 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Control and Instrumentation Fuel Design	
GDA Issue Reference	**GI-AP1000-FS-04**	**GDA Issue Action Reference**	**GI-AP1000-FS-04.A1**
GDA Issue	To examine the feasibility of enhancing the flux protection on the AP1000 to provide automatic and diverse protection against frequent adverse power distribution faults possibly using the current design of in-core instrumentation.		
GDA Issue Action	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. Westinghouse is proposing to use the BEACON computer code as an on-line monitoring system to provide continuous indications of power distributions and key safety parameters. These surveillances are used to alarm conditions where the margin to key safety limits becomes unacceptable. The software reliability of such complex computer codes is not considered sufficient in isolation to provide this function to a high level of reliability. In addition, BEACON is not integrated into the protection system. In Sizewell B, the core power profile and margin to safety limits is monitored by the reactor primary protection system using a matrix of ex-core detector importance factors. These factors are subject to a rigorous QA process independent of the core design process and validated against flux maps. Given the rigor with which the primary protection system software is validated, the monitoring of core power peaking and of the margin to safety limits is carried out with a high degree of confidence. The situation was a requirement placed on Sizewell B as part of the licensing process, and is considered relevant good practice within the UK. ONR requires that Westinghouse demonstrate whether it is reasonably practicable to provide extra protection against adverse power-distribution faults using the current design of in-core instrumentation. It is not considered credible that this can be achieved using a system relying solely on a software system including a reactor physics code similar to that of BEACON. The response to this GDA issue should include an ALARP assessment, which demonstrates whether it is reasonably practicability to provide additional protection on the peak linear and the margin to CHF, based upon in-core instrumentation. Furthermore, the assessment should consider the use of rod freeze protection to ensure that limits on shutdown margin are not violated. The design for any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PROVISION OF ENHANCED AND DIVERSE FLUX PROTECTION TO PROTECT AGAINST ADVERSE POWER DISTRIBUTION FAULTS

GI-AP1000-FS-04 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Control and Instrumentation Fuel Design		
GDA Issue Reference	**GI-AP1000-FS-04**	**GDA Issue Action Reference**	**GI-AP1000-FS-04.A2**
GDA Issue Action	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. Westinghouse has demonstrated that the hot leg temperature trip on the DAS provides diverse protection against RCCA bank withdrawal faults occurring at power. However, the responses provided do not demonstrate diverse protection against excessive increase in secondary steam flow faults greater than 10% flow or demonstrate diverse flux protection for rod misalignment faults up to and including rod drop faults. ONR requires Westinghouse to demonstrate that there is automatic diverse protection against these frequent faults. In seeking to demonstrate adequate protection for these faults, Westinghouse should consider the feasibility of using the current design of in-core instrumentation enhanced in accordance with the previous action of this GDA issue. The response to this GDA issue should include a transient analysis assessment for the excessive increase in secondary steam flow fault at full power and rod misalignment faults including rod drop faults in which the ex-core detectors are assumed to be ineffective due to a common mode failure. The design for any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

POTENTIAL ENHANCEMENTS TO THE DIVERSE SAFETY INJECTION SYSTEM

GI-AP1000-FS-05 REVISION 1

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Mechanical Engineering Control and Instrumentation Probabilistic Safety Assessment Human Factors		
GDA Issue Reference	**GI-AP1000-FS-05**	**GDA Issue Action Reference**	**GI-AP1000-FS-05.A1**
GDA Issue	Westinghouse is to examine whether it is reasonably practicable to enhance the design of the RNS system in its role as the diverse safety injection system on the AP1000.		
GDA Issue Action	Westinghouse is to examine whether it is reasonably practical to enhance the design of the RNS system in its role as providing a diverse means of safety injection on the AP1000. Westinghouse will have to perform an ALARP review identifying potential options for enhancing the design of the RNS system. The options considered include automating its actuation using an appropriately classified (C&I) system that is diverse from the PMS, segregating the water supply of the system from the IRWST, and increasing the pressure head of the RNS system. It is accepted that the RNS system is not the principal means of fulfilling the nuclear safety function and so an A2 classification for the system should suffice for this function. In considering the options, Westinghouse will have to identify the potential safety benefits of the different options using both design basis transient analysis and probabilistic analysis techniques. If any design modifications are proposed for the AP1000, they will have to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

VALIDATION OF THE IRWST COOLING FUNCTION FOR THE PRHR

GI-AP1000-FS-06 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment	
GDA Issue Reference	**GI-AP1000-FS-06**	**GDA Issue Action Reference**	**GI-AP1000-FS-06.A1**
GDA Issue	Westinghouse is to provide validation evidence that the IRWST is functionally capable cooling the passive residual heat removal (PRHR) during intact circuit faults for 72 hours.		
GDA Issue Action	• Westinghouse is to provide validation evidence that the IRWST is functionally capable cooling the passive residual heat removal (PRHR) during intact circuit faults for 72 hours. Or • Propose a design change to rectify the situation. No design basis transient analysis is presented within the DCD to demonstrate that the IRWST and PCS has the functional capability to act as an adequate heat sink to the PRHR when the latter is performing its post-trip heat removal safety function following an intact circuit fault. For this reason, Westinghouse is to provide explicit transient analysis using design basis techniques to demonstrate the functional capability of these systems. If relevant, Westinghouse needs to identify any bounding single failure. The analysis needs to be performed on a conservative basis with justification given for any modelling assumptions. Where possible, the analytical models should be validated by comparison with appropriate experiments or tests. The validation should be of the model as a whole or, where this is not practicable, on a module basis, against experiments that represent as closely as possible the expected plant conditions. Interpretation of experiments should take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of any analytical model should be identified. In particular, Westinghouse is required to provide validation evidence supporting the claimed condensate return efficiency of 95% to the IRWST and to demonstrate that the effect of containment pressure on the effectiveness of the IRWST cooling function for the PRHR has been taken into account in the safety analysis for loss of feed faults. The resultant transient analysis studies will need to be incorporated within the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SAFETY CASE FOR SHUTDOWN FAULTS

GI-AP1000-FS-07 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-FS-07**	**GDA Issue Action Reference**	**GI-AP1000-FS-07.A1**
GDA Issue	Westinghouse is required to provide a fully integrated design basis safety case for shutdown faults in the PCSR. The safety case for shutdown faults needs to be reflected in and supported by the Fault Schedule, also to be reported in the PCSR.		
GDA Issue Action	Westinghouse is required to provide a fully integrated design basis safety case for shutdown faults in the PCSR. The safety case for shutdown faults needs to be reflected in and supported by the Fault Schedule, also to be reported in the PCSR. An acceptable design basis safety case for shutdown faults requires Westinghouse to provide more than is currently presented in the EDCD and the response to RO-AP1000-54 (UKP-GW-GL-077 Rev 0). Shutdown faults need to fully integrated into the PCSR. If the available at-power design basis analyses (i.e. the thermal hydraulic analysis, radiological consequences and claims on SSCs) are assumed to bound or apply to shutdown faults then this needs to be clearly stated in the PCSR, justified as necessary, and initiating fault frequencies updated accordingly. Fault sequences which are significantly different in terms of consequences or claims on SSCs from their at-power equivalents need to be considered separately, but with the full rigour expected for design basis analysis (i.e. SAPs FA.4 to FA.9). This includes consideration of limiting single failures, demonstration of diversity for frequent faults and discussion of the consequences. It is expected that the worst normally permitted (under Tech Specs) configuration of equipment should be clearly stated for faults in each applicable shutdown mode in accordance with SAP FA.6. Faults during refuelling modes of operation need to be covered in the PCSR. The safety case for RNS pipe breaks outside of containment needs to be completed with arguments, transient analysis, design change proposals etc. presented in and referenced from the PCSR as necessary. The safety case for shutdown faults needs to be reflected in and supported by the Fault Schedule, also to be reported in the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

FAULT SCHEDULE FOR AP1000

GI-AP1000-FS-08 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	All		
GDA Issue Reference	**GI-AP1000-FS-08**	**GDA Issue Action Reference**	**GI-AP1000-FS-08.A1**
GDA Issue	Westinghouse is required to present their Fault Schedule to ONR and support as necessary ONR's subsequent assessment of it. The Fault Schedule is to be updated as appropriate following assessment by ONR and to incorporate any changes/additions to the AP1000 safety case resulting from GDA Issues.		
GDA Issue Action	Westinghouse is required to present their Fault Schedule to ONR and support as necessary ONR's subsequent assessment of it. The Fault Schedule is to be updated as appropriate following assessment by ONR and to incorporate any changes/additions to the AP1000 safety case resulting from GDA Issues. A definitive Fault Schedule was not provided to ONR for assessment in GDA Step 4. At the end of March 2011, Westinghouse provided ONR with Rev 0 of the PCSR which included a new Fault Schedule. However this has not been assessed to date. Westinghouse shall develop a programme to facilitate ONR's assessment of this crucial part of the PCSR. It will allow for: ▪ Westinghouse to present their methodology and intent followed to produce the Fault Schedule; ▪ Westinghouse to present to ONR the extent and scope of the Fault Schedule and their plans to update it in the future; ▪ Sufficient time for ONR to assess the Fault Schedule; ▪ Westinghouse to address any comments on the adequacy of the Fault Schedule; ▪ Any revisions to the Fault Schedule as result of GDA Issues, design modifications or changes to the PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

Further explanatory / background information on the GDA Issues for this topic area can be found at:	
GI-UKEPR-FS-01 Revision 0	Ref. 135.
GI-UKEPR-FS-02 Revision 0	Ref. 136.
GI-UKEPR-FS-03 Revision 0	Ref. 137.
GI-UKEPR-FS-04 Revision 0	Ref. 138.
GI-UKEPR-FS-05 Revision 1	Ref. 139.
GI-UKEPR-FS-06 Revision 0	Ref. 140.
GI-UKEPR-FS-07 Revision 0	Ref. 141.
GI-UKEPR-FS-08 Revision 0	Ref. 142.