HSE

Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 FAULT STUDIES ASSESSMENT OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/018-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This report presents my findings for the Fault Studies assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) and its supporting Design Control Document (DCD) undertaken as part of Step 3 of the Health and Safety Executive (HSE) Generic Design Assessment (GDA) process. It provides an overview of the safety case; the standards and criteria adopted in the assessment; and the assessment of the claims and arguments provided within the safety case.

It should be recognised that the technical assessment in the fault analysis area only commenced part way through the Step 3 GDA process. For this reason, the scope of the assessment has had to be limited in extent, concentrating on reviewing the core design, the design basis analysis and certain aspects of the severe accident analysis. In Step 4, the scope of the assessment will be extended to examining the thermal hydraulic analysis performed in support of the Probabilistic Safety Analysis (PSA) success criteria. The validation of the computer codes will also be reviewed in detail and in selected cases independent confirmatory analyses will be performed.

I conclude that Westinghouse has provided a safety analysis that is generally satisfactory but there are still some areas where I believe that further work and additional information is required. Specific findings include:

- There is a need to demonstrate that the list of design basis initiating events is complete including faults at shutdown and on the spent fuel pool. The list of design basis initiating faults will need to be reconciled with those of the PSA. A design basis safety case is required for each fault.
- There is a need for Westinghouse to review all design basis initiating events with a frequency of greater than $1x10^{-3}$ per year and demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each safety function. The single failure criterion also needs to be extended to include passive failures.
- A radiological consequence assessment needs to be performed for each design basis fault against Target 4 of the safety assessment principles.
- The proposal to use the BEACON reactor physics code to demonstrate on-line compliance with the fuel safety technical specifications will need to show that an independent method exists for the operator to ensure compliance.
- There is a need to demonstrate that the 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 needs to be considered.
- Anticipated Transient Without Trip (ATWT) faults need to be included within the design basis. An As Low As Reasonably Practicable (ALARP) justification for not installing an emergency boration system will also be required.
- For each fault, Westinghouse needs to provide evidence that the plant can reach a safe shutdown state from a controlled state.
- The assessment of large-break loss-of-coolant accidents compares the fuel cladding temperatures expected against safety limits. This analysis needs to include detailed consideration of the potential for fuel channel blockage caused by features of the transient such as plastic buckling of spacer grids.
- Westinghouse has made a case for the retention of core material in the vessel should the core melt in a severe-accident. The modelling of melt progression is currently a controversial area with significant uncertainty. Further examination of this research is required.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
ATWT	Anticipated Transient without Trip
BMS	(Nuclear Directorate) Business Management System
BSL	Basic Safety Level
CAMP	Code and Maintenance Programme
CCW	Component Cooling Water System
CFD	Computational Fluid Dynamics
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
DCD	Design Control Document
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DVI	Direct Vessel Injection
ECS	Emergency Charging System
GDA	Generic Design Assessment
HHSI	High Head Safety Injection
HSE	The Health and Safety Executive
HSL	The Health and Safety Laboratory
IAEA	The International Atomic Energy Agency
IFBA	Integral Fuel Burnable Absorbers
IRWST	In-containment Refuelling Water Storage Tank
LBLOCA	Large Break Loss of Coolant Accident
LOCA	Loss of Coolant Accident
MAAP	Modular Accident Analysis Program
MDEP	Multi-National Design Evaluation Programme
MOX	Mixed Oxide Fuel
ND	The (HSE) Nuclear Directorate
PCI	Pellet-Clad Interaction
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PMS	Protection and Monitoring System

LIST OF ABBREVIATIONS

POSRV	Pilot Operated Safety Relief Valves
PPS	Primary Protection System
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal Heat Exchanger
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report
PSRV	Pressuriser Safety Relief Valves
PWR	Pressurised Water Reactor
PXS	Passive Core Cooling System
RAPFE	Radial Averaged Peak Fuel Enthalpy
RCCA	Rod Control Cluster Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RIA	Regulatory Issue Action
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
ROAAM	Risk-Oriented Accident Analysis Methodology
RP	Requesting Party
RPV	Reactor Pressure Vessel
SAP	Safety Assessment Principle
SBLOCA	Small Break Loss of Coolant Accident
SFS	Spent Fuel Cooling System
SFP	Sandia Fuel Project
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SPS	Secondary Protection System
TEDE	Total Effective Dose Equivalent
TQ	Technical Query
US NRC	United States Nuclear Regulatory Commission
WABA	Wet Annular Burnable Absorber

TABLE OF CONTENTS

1 INTRODUCTION

1 This report presents my findings for the Fault Studies assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) and it's supporting Design Control Document (DCD) (Ref. 2) which has been undertaken as part of Step 3 of the Health and Safety Executive (HSE) Generic Design Assessment (GDA) process. This assessment has been performed in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 3) and its associated guidance document G/AST/001 (Ref. 4). G/AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 5) have been used as the basis for the assessment of the Fault Studies aspects associated with the AP1000 design.

2 Ultimately, the goal of assessment is to reach an independent and informed judgement on the adequacy of a nuclear safety case. This report forms an initial view based on a limited sampling.

3 During the Step 2 assessment (Ref. 6) a high level review of the Westinghouse AP1000 Preliminary Safety Report (PSR) (Ref. 7) was performed based upon a comparison of the claims made in the PSR against the guidance on good practice provided by the SAPs. The objective of the Step 3 assessment is to review the safety aspects of the AP1000 in a more detailed way by examining the claims and arguments made in the preliminary Westinghouse PCSR (Ref. 1) and the supporting DCD (Ref. 2). In considering the SAPs to be addressed during Step 3, I have exercised my technical judgement in selecting the appropriate SAPs to be used in the assessment and in the level of detail to which the assessment has been taken. The focus has been on the analysis of plant failures leading to the largest hazards / risks and the most limiting faults within the design.

4 It should be recognised that the technical assessment in the Fault Studies area only commenced part way through the Step 3 GDA process. For this reason, the scope of the assessment has been more limited than some of the other technical areas and has primarily concentrated upon reviewing the core design, the design basis analysis and certain aspects of the severe accident analysis. Given the resources now available, I am confident those areas not reviewed in Step 3 will be adequately covered during Step 4. For example, in Step 4, the scope of the assessment will be extended to examining the thermal hydraulic analysis performed in support of the Probabilistic Safety Assessment (PSA) success criteria. Assessment during Step 4 will also address the adequacy of the evidence supporting the claims and arguments assessed within Step 3. In particular, the validation of the computer codes which play a significant part of the analyses will be reviewed in detail and in selected cases independent confirmatory analyses will be commissioned from technical support contractors.

5 The use of Mixed Oxide Fuel (MOX) within the reactor core and the fuel handling facilities has been excluded from the scope of this GDA Fault Studies assessment. Westinghouse has been asked to produce a Fault Schedule for the AP1000. A draft version of this document has been provided to ND during Step 3 but not in time to form part of my assessment.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

6 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 probabilistic risk assessment

(PRA)[1] demonstrates that the residual risk from accidents beyond the design basis has been reduced to as low as is reasonably practicable.

7 In order to achieve these objectives, Westinghouse claims 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 safety systems will operate automatically when required regardless of the availability of off-site power supplies and the normal generating system. 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 safety systems avoids the use of 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 are 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 system maintains the integrity of the containment vessel by ensuring that the pressure and temperature of the containment remains within the appropriate design limits for both design basis and severe accident scenarios.
- The reactor vessel and its insulation systems are designed to promote ex-vessel cooling and to achieve in-vessel melt retention in the unlikely event of failure of normal safety injection. With the reactor vessel intact and debris retained in the lower head, phenomena such as molten corium-concrete interaction and ex-vessel steam explosions are prevented.

[1] The discipline of “Probabilistic Risk Assessment” (PRA) is commonly referred to by its equivalent name “Probabilistic Safety Analysis” or PSA in the UK. However, as a key Westinghouse reference (Ref. 9) has “Risk Assessment” in its title, PRA has generally been used in this report.

2.2 Standards and Criteria

8 Judgements have been made against the 2006 HSE SAPs for Nuclear Facilities (Ref. 5). In particular, the fault analysis and design basis accident SAPs (FA.1 to FA.9), the PSA SAPs (FA.10 to FA.14), 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.3, EKP.5, EDR.1 to EDR.4, ESS.2, ESS.4, ESS.6 to ESS.8, ESS.11, ERC.1 to ERC.4, EHT.1 to EHT.4) have been considered. The Requesting Party (RP) has assessed the safety case against its own design requirements.

9 Comparisons against the SAPs have been made throughout the main text of this report against specific aspects of the AP1000 design and safety case. In addition, a summary of my assessment of Westinghouse's safety case for the AP1000 against the SAPs identified above is provided in Table 1.

2.3 Nuclear Directorate Assessment

10 The Fault Studies assessment of AP1000 has been divided into three sections covering 1) nuclear design of reactor core design, 2) fault analysis and 3) severe accident analysis.

11 Following on from the discussion of these three specific areas, I have reviewed the Step 2 findings in the Fault Studies area, the use of overseas regulators information, relevant research to the Fault Studies assessment of the AP1000. I have also summarised the Regulatory Observations (ROs) that I intend to raise as a result of my Step 3 assessment and my current assessment plans for Step 4.

2.3.1 Nuclear Design of Reactor Core

2.3.1.1 Summary of Requesting Party's Safety Case

12 The nuclear design of the core affects the behaviour of the reactor during normal operation and also during fault conditions and so is of fundamental importance to the safety case. In particular, the control of reactivity in the core has a direct bearing on reactor safety. Key aspects of the design that need to be considered are the core power distribution, the effects on the moderator temperature reactivity coefficients of the soluble boron concentration, the adequacy of the shutdown margin, and the stability of the core against spatial power oscillations.

13 The nuclear design aspects of the AP1000 core are presented within Section 4.3 of Chapter 4 of the DCD. The basis of the Westinghouse safety case is to ensure that the design of the core meets the following design criteria:

- the core power distribution limits related to fuel integrity are met for normal operation and operational transients through conservative design and are maintained by the action of the control system;
- the fuel will not operate with a power distribution that would result in exceeding the Departure from Nucleate Boiling (DNB) design basis for normal operation and operational transients and for faults of moderate frequency including the maximum overpower condition;
- under abnormal conditions, including the maximum overpower condition, the peak linear heat rate will not cause fuel melting;
- fuel management will be such as to produce values of fuel rod power and burn-up consistent with the assumptions in the fuel rod mechanical integrity analysis;

- the fuel will not be operated at peak linear heat rate values greater than those found to be acceptable within the body of the safety analysis under normal operating conditions;
- the maximum reactivity rate due to withdrawal of rod cluster control assemblies or grey rods cluster assemblies or by boron dilution is limited by plant design, hardware, and basic physics. During normal operation, the maximum controlled reactivity insertion rate is limited. The maximum reactivity change rate for accidental withdrawal of two control banks is set such that the peak linear heat rate and the departure from nucleate boiling ratio limitations are not challenged;
- for the initial fuel cycle, the fuel temperature coefficient will be negative, and the moderator temperature coefficient of reactivity will be negative for power operating conditions;
- the minimum shutdown margin as specified in the technical specifications (which has yet to be defined) is required in all operating modes;
- in analyses involving reactor trip, the single, highest worth rod cluster control assembly is postulated to remain untripped in its full-out position (stuck rod criterion);
- when fuel assemblies are in the pressure vessel and the vessel head is not in place, k_{eff} will be maintained at or below 0.95 with the control rods and soluble boron. Furthermore, the fuel will be maintained sufficiently subcritical that removal of the Rod Cluster Control Assemblies (RCCA) will not result in criticality;
- the core will be stable to power oscillations in the fundamental mode, and;
- spatial power oscillations within the core with a constant core power output, should they occur, can be reliably and readily detected and suppressed.

2.3.1.2 ND Assessment

14 The design of Pressurised Water Reactor (PWR) cores is a well established technology. The changes made to the AP1000 core when compared with the earlier generation of Westinghouse reactor cores are relatively modest extrapolations on designs that are known to have worked well. For this reason, I have elected to perform only a high level review of Westinghouse's design criteria for the Step 3 assessment against a selection of the more relevant parts of the reactor core SAPs ERC.1 to ERC.4. A more detailed assessment will be performed in Step 4. It should be noted that an assessment of the fuel design is provided in a separate report (Ref. 8) and discussion of the requirements of ERC.2 with regard to the provision of a diverse shutdown system is deferred to the discussion of Anticipated Transients without Trip (ATWT) events below.

15 The design intent of the AP1000 core is to reduce the maximum soluble boron concentration in the core at the start of cycle by using an Integral Fuel Burnable Absorber (IFBA) in the form of boron carbide coated fuel pellets and Wet Annular Burnable Absorbers (WABA). The IFBA approach is similar in concept to the gadolinium doping currently used at Sizewell B. The WABA technology was employed in the early cycles of Sizewell B and did not raise any particular issues except perhaps the requirement for long-term disposal of additional core components. Reactivity control in the short term is managed using a mechanical shim consisting of a bank of 'grey' control rods that contain a significantly reduced quantity of absorber material. These grey rods are used to control reactivity changes during load manoeuvres so minimising the need to change boron concentration using the Chemical and Volume Control System (CVS).

16 Westinghouse claims that the reduction in initial boron concentration at the start of cycle due to the presence of the burnable poisons ensures that the moderator temperature coefficient of reactivity for AP1000 is always negative for at power conditions. This claim

will need to be reviewed in detail against the requirements of SAP ERC.3 in Step 4 since this parameter has a significant effect on the response of the AP1000 to an ATWT event. In particular, it is important to ensure that both the fuel and the moderator temperature reactivity coefficients are sufficiently negative throughout the cycle length to protect against an ATWT event following a boron dilution fault at hot zero power. The feasibility of identifying a suitable limit and condition for inclusion within the technical specifications so as to ensure an adequately negative moderator temperature coefficient for the full cycle length using burnable poisons will be explored with Westinghouse in Step 4.

17 The design requirements to meet 1) the stuck rod criterion and 2) to ensure the fuel will be maintained sufficiently subcritical such that removal of a RCCA will not result in criticality would appear to meet the requirements of ERC.1 although in the latter case there is a need to apply an appropriate uncertainty allowance. This issue will be discussed with Westinghouse during Step 4 although it is noted that in practice for the assessment of shutdown margin against the stuck rod criterion the shutdown margin for AP1000 is likely to be greater than that for Sizewell B.

18 The negative fuel and moderator temperature coefficients discussed above also help with reactor stability in normal operation. Due to the negative power coefficient of reactivity, PWR cores are inherently stable to oscillations in total power. However, xenon induced spatial oscillations mainly in the axial plane, but also the X-Y plane, are possible. The size of the AP1000 core is smaller than Sizewell B in the X-Y plane but Westinghouse concedes that because the length of the AP1000 core at 4.27 m (14 ft) is longer than many previous cores including Sizewell B (3.66 m or 12 ft), the reactor will be slightly less stable in the axial direction. For this reason, the axial stability index will become zero earlier in cycle. Westinghouse claims that the control banks provided are sufficient to dampen any xenon oscillations that may occur. The implications of this in terms of the demand placed on the operator and the control system of grey rods will need to be explored further in Step 4 in order to ensure that the requirements of SAP ERC.3 are met.

19 A related matter is that Westinghouse is proposing to use the BEACON computer code as an online monitoring system to provide continuous indications of current power distributions as required by SAP ERC.4 and to provide guidance to the plant operator as to the timing and most appropriate actions to maintain stable axial power distributions. It is understood that the intention is to use BEACON to eliminate the need for compliance with many of the core related technical specifications. In my judgement, this proposal represents a serious concern unless an independent means exists for the operator to verify that the reactor remains compliant with the technical specifications due to concerns about the software reliability of such complex computer codes when applied to reactor control applications. An RO will be raised requiring Westinghouse to demonstrate that a diverse means of demonstrating compliance with the technical specifications will be employed.

2.3.2 Fault Analysis

20 The design basis accident analyses for the AP1000 are presented within Chapter 15 of the DCD 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. 9). The latter also includes an assessment of faults that occur during shutdown operations for which no design basis analysis is presented within the DCD. 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 the shutdown faults, additional analysis will be required.

21 The design basis analysis presented in Chapter 15 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.

22 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 Nuclear Regulatory Commission (US NRC) in 10 CFR 50.34. These differ from the dose limits given in SAP T.4. Westinghouse is currently developing a Fault Schedule and so it is not possible to identify the initiating frequency assigned to each initiating fault at this time so comparison with SAP Target 4 is difficult.

23 The categorisation scheme discussed above is based upon the ANSI N18.2 standard (Ref. 10), which dates from 1973. This guide has been superseded by a latter version produced in 1983 (Ref. 11). 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. In the UK, it is considered good practice to consider any fault sequence with a frequency greater than 1 x 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 less than 1 x 10^{-5} per demand, in practice this means that for any initiating frequency greater than 1 x 10^{-2} per year (and in practice for most initiating frequencies greater than 1 x 10^{-3} per year) a diverse safety system 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, an RO will be raised requiring Westinghouse to review all design basis initiating events with a frequency of greater than 1 x 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.

24 The safety functions that need to be reviewed for frequent faults include those required to move the reactor from the controlled state to the safe shutdown state following any design basis fault. Indeed, Westinghouse has not provided any discussion or analysis within the DCD of how the reactor will move from the controlled state to the safe shutdown state. For this reason, an RO will be raised requiring Westinghouse to provide evidence that the plant can reach a safe shutdown state following any design basis accident. This extension to the design basis analysis will need to be included within a revision of the PCSR.

25 In particular, there is a need to demonstrate that diverse protection is provided for the long term hold down of the core following a reactor trip and the decay of xenon. In the case of Sizewell B, the Chemical Volume and Control System (CVCS) is qualified to safety system standards and automatically controls boron levels following reactor trip to ensure an adequate shutdown margin is maintained. Should the CVCS fail to operate, then the Emergency Charging System (ECS), which is diverse from the CVCS, and which is also qualified to safety system standards will automatically start to inject boron. The ECS is driven by steam turbines and so does not require the supply of electrical power

from the essential AC electrical system. In contrast, the CVS on the AP1000 is not qualified to safety system standard and it is not obvious that the Core Make-up Tanks (CMTs), which have the capability to inject borated water into the core, will automatically provide this safety function should the CVS fail to operate. This issue will need to be explored further with Westinghouse in Step 4.

26 The design basis analyses presented in Chapter 15 of the DCD also considers faults according to the following fault types:

- increase in heat removal from the primary system;
- decrease in heat removal by the secondary system;
- decrease in Reactor Coolant System (RCS) flow rate;
- reactivity and power distribution anomalies;
- increase in reactor coolant inventory;
- decrease in reactor coolant inventory;
- radioactive releases from a subsystem or component, and;
- anticipated transients without scram (i.e. trip).

27 Although ATWT is listed, Westinghouse does not consider it to be within the design basis and so no analysis is presented under this item. This list of design basis initiating events can be compared with the list of design basis initiating events considered for Sizewell B (Ref. 12):

- reactor trip faults;
- increase in heat removal faults;
- decrease in heat removal faults;
- electrical supply faults;
- decrease in RCS flow rate faults;
- reactivity and power distribution anomalies;
- increase in reactor coolant inventory faults;
- decrease in reactor coolant inventory faults;
- other (support) system faults;
- control and protection faults, and;
- faults affecting non-core sources of radioactivity.

28 In the case of Sizewell B, ATWT events are explicitly included within each fault category as a failure to trip sequence and so there is no need for a separate section covering them. It is noticeable that the AP1000 design basis list does not include spurious reactor trip, electrical supply faults, support system faults and control and protection faults. It may well be that this is a presentational issue and that these faults are effectively included within the other fault categories. However, this is not clear directly from inspection of the list.

29 The AP1000 list of initiating events is again based on the prescriptive ANSI N18.2 standard (Ref. 11), dating from 1973. SAP FA.2 requires that the process for identifying initiating faults should be systematic, auditable and comprehensive since this is considered to represent modern practice in the UK. It is noted that Chapter 2 of the PRA (Ref. 9) provides a list of initiating events which appears to be based upon an attempt at a systematic assessment of the failure modes of the structures, systems and components

comprising the AP1000. The PRA therefore considers failures in the pressure boundary (loss of coolant accidents), frontline systems (transients), support systems (including electrical systems) and instrumentation and control systems. The transient category includes spurious reactor trip. In principle, any initiating event identified in the PRA should be included within (or bounded by) a design basis initiating event unless it is screened out on the basis of low frequency as is acknowledged by SAP FA.5. In order to demonstrate that the list of design basis initiating events considered within the PCSR is as comprehensive as possible, I consider that it is necessary to reconcile the Westinghouse list of design basis initiating events with the Westinghouse list of PSA initiating events. An RO will be raised requiring Westinghouse to perform such an assessment in support of a future revision of the PCSR.

30 SAP FA.3 requires that fault sequences should be developed from the initiating faults and their potential consequences analysed. In order to assess whether this has been achieved, it is necessary to review each fault category on an individual basis. In the following sections, the design basis analyses performed by Westinghouse with the aim of demonstrating fault tolerance, as required by FA.4, will be reviewed in turn for each of the following fault categories:

- increase in heat removal from the primary system;
- decrease in heat removal by the secondary system;
- 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);
- ATWT;
- spent fuel pool faults;
- shutdown faults;
- internal faults, and;
- external faults.

31 No attempt has been made to assess the PRA fault sequences or the Fault Studies aspects of the internal and external hazards analyses at this time although the latter are listed above for completeness. These areas will be reviewed as part of Step 4 of the GDA assessment.

2.3.2.1 Increase in Heat Removal Faults

2.3.2.1.1 Summary of Requesting Party's Safety Case

32 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 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 Reactor Pressure Vessel (RPV) to a high pressure at 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 steam generator tube ruptures which would increase the loads on the containment. 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.

33 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 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, isolate the steam generators to reduce the rate of reactor cool-down, initiate post-trip cooling using the Passive Residual Heat Removal (PRHR) heat exchanger and initiate the flow of borated water from the CMTs to ensure an adequate shutdown margin.

34 In performing the transient analysis, Westinghouse assumes that the most reactive RCCA fails to enter the core. Sensitivity studies have been performed on the effects of the availability of offsite power following reactor trip (which depending on the assumption, can result in the tripping of the Reactor Coolant Pumps [RCPs]), 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 range of faults considered.

2.3.2.1.2 ND Assessment

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

- 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;
- inadvertent operation of the PRHR heat exchanger.

36 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. I have chosen to sample the last three faults listed above on the grounds that steam system piping failure is the most limiting fault according to Westinghouse, inadvertent opening of a relief or safety valve is 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.

37 In this preliminary assessment performed for Step 3 of the GDA only the design basis analyses have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such faults performed to underpin the success criteria for the PRA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed. In addition, no assessment has yet been made of containment integrity aspects of these faults, which are reported separately in Chapter 6 of the DCD. This work will be performed as part of Step 4.

38 To aid my judgement I have benchmarked the analysis approach adopted by Westinghouse against some scoping analysis performed in support of the original Sizewell B PCSR (Ref. 14) as an exemplar of relevant good practice in the UK. I have also been supplied with a technical paper by Westinghouse (Ref. 15) justifying some of its methodological assumptions for performing steam line break analyses. These documents help give confidence in the validation of the computer codes used to perform the analysis. However, no attempt has been made within Step 3 to make a detailed assessment of these codes against the validity of assurance SAPs FA.17 to FA.22. Again, such work will be performed as part of Step 4.

39 The steam system piping failure assessment assumes the rupture of a main steam line. Westinghouse is still in the process of producing a Fault Schedule for the AP1000 and so it is not possible to explicitly state what initiating frequency is being assumed for this event. However, for Sizewell B (Ref. 14) a main steam line rupture inside containment was assumed at a frequency of 1 x 10^{-4} per year while one outside containment was assumed at 1 x 10^{-3} per year. Such frequencies would appear to be consistent with the assumption of a Condition III / IV event being made by Westinghouse. 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.

40 Westinghouse has indeed treated the fault as being within the design basis and identified what it considers to be the most onerous single failure (failure of a discharge valve on one of the CMTs). Clearly, 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 such that 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 effected Steam Generator (SG) is not assumed to be isolated so bounding any single failure of the main steam isolating valves. The protection signals that are claimed are all based upon 2-out-of-4 voting logic.

41 No sensitivity studies to break size and power level are presented within the DCD. However, the Sizewell B report (Ref. 14) does present such parametric sensitivity studies. 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 the larger breach sizes starting the transient calculation from the hot zero power condition is bounding in terms of the minimum Departure from Nucleate Boiling Ratio (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. 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. Westinghouse should be requested to produce further sensitivity studies to confirm the conclusions of its analysis in Step 4.

42 Westinghouse has not presented the minimum DNBR results for the steam line break case in the DCD, merely stating that it meets the design basis limit when judged against the W-3 correlation (Ref. 2). Westinghouse has chosen the DNBR design basis limit for the low pressures associated with cool-down faults to be 1.45. This is low compared with the value of 2.0 that is assumed at Sizewell B (Ref. 14) which 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 low pressure. This issue will need to be explored further with Westinghouse during Step 4.

43 The results of the Westinghouse analyses are summarised in Figures 15.1.5-2 and 15.1.5-7 of the DCD 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. 14) which predicts a 14% peak return to power and a minimum DNBR of 2.27. These results are not necessarily surprising since the AP1000 is known to possess a larger shutdown margin than Sizewell B. In the case of AP1000, borated water is injected from the CMTs whereas Sizewell B relies upon the High Head Safety Injection (HHSI) system. The increase in shutdown margin is due to the size of the AP1000 reactor core which is smaller than Sizewell B and yet it contains the same number of shutdown RCCAs. For Sizewell B, the minimum end of life shutdown margin with the worst RCCA stuck in its fully withdrawn position is 1.3 Niles (Ref. 14) while the design basis minimum shutdown limit for AP1000 from Table 4.3-3 of the DCD appears to be 1.6 Niles.

44 Westinghouse concedes that a stuck open relief or safety valve is 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 to ensure that a design basis sequence frequency of less than 1 x 10^{-7} per year (Ref. 13) is achieved for an individual fault given the requirements of SAPs EDR.2 and EDR.3 for the consideration of common mode failure. Westinghouse does not consider common mode failure of a whole system in coincidence with an initiating event to be within its design basis but does require that the single failure criterion is met.

45 There is therefore a need for Westinghouse to consider the following sequence of events that are claimed to protect against a stuck open relief valve fault and demonstrate either a diverse safety system, qualified to appropriate standard, or the inherent characteristics of the plant will provide protection for each of the relevant safety functions:

- fault detection;
- reactor trip;
- initiation of the CMTs;
- initiation of the PRHR;
- isolation of feedwater and steam systems.

46 As an example, Westinghouse needs to consider a sensitivity study in which common mode failure of the CMTs to inject borated water is assumed and demonstrate that in the case of cool-down faults, the fuel does not enter DNB. It should be noted that Sizewell B (Ref. 14) is provided with an emergency boration system that helps protect against failure of the HHSI. This is a specific example of the more general finding requiring a demonstration of diverse safety system, qualified to an appropriate standard, for each safety function for all frequent faults and for which the need for an RO has already been identified. It should also be noted that the Sizewell B analysis (Ref. 14) also 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 x 10^{-7} per year (Ref. 13).

47 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. 14) 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 claims the digital Protection and Monitoring System (PMS) monitors the cool leg temperatures and can

correct for this effect. This claim may need to be reviewed as part of the Step 4 assessment.

48 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 feature. Westinghouse has correctly identified that this initiating event needs to be included in the list of cool-down events within the design basis analysis. However, this raises the question of whether there are other initiating events that should be considered within the design basis because of changes in the AP1000 design compared with the earlier generation of PWRs. No reference is given as to how this initiating event was identified. This reinforces the need for the RO requiring Westinghouse to reconcile the list of design basis initiating events with those that should have been systematically identified within the PRA.

49 Following inadvertent initiation of the PRHR, the core power increases to about 120% power from full power (assuming manual control of the RCCAs) before stabilising at 1.08% power as illustrated in Fig 15.1.6-2 of the DCD. Fig 15.1.6-6 shows that the minimum DNBR is about 1.9 for this transient in which the pressure remains comfortably within the range of validity of the WRM-2M correlation. 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, where the need is to maximise the heat removal capability.

50 Within Step 3 no attempt has been made to review the radiological assessment supporting the design basis assessment for these faults although it is known that the assessment has been made against US criteria. An RO will be raised requiring that such an assessment is made against the UK requirements given in SAPs FA.3, FA.7 and Target 4 for resolution during Step 4 although I judge that this is probably a methodological issue that is unlikely to lead to the need for additional protection measures for these faults.

51 The Westinghouse analysis uses the LOFTRAN computer code to model the system transient while the VIPRE-01 computer code is used to determine whether DNB occurs. The validation evidence for these two codes has not been assessed in Step 3 of the GDA against SAPs FA.17 to FA.22. However, confidence can be gained by noting that the LOFTRAN computer code was also used to perform the analysis in Sizewell B report (Ref. 14). Nevertheless, the LOFTRAN code has subsequently been modified to incorporate the modelling of the passive features on AP1000. The Sizewell B analysis used THINC-IV computer code to perform the DNB analysis with VIPRE used for independent checking. A Technical Query (TQ) has been raised covering the allowance for uncertainties within the DNB correlation for the low pressure conditions that occur during these faults. For the Step 4 assessment, I will review the validation evidence supporting the calculational route.

52 No discussion is presented within the analyses about the possibility of consequential SGTR failures during a steam line break. 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 as high as 1 x 10^{-1} per demand. If such high frequencies are reflected within AP1000 design, there is a case for considering such sequences to be within the design basis according to SAP FA.5. This issue will need to be explored further with Westinghouse during Step 4 of the GDA once the Fault Schedule is available. There is also no discussion provided of how the reactor will be brought from the controlled state to the safe-shutdown state within the analysis.

2.3.2.2 Decrease in Heat Removal Faults

2.3.2.2.1 Summary of Requesting Party's Safety Case

53 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 through the pressuriser since 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 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 then 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 for safety relief valves to lift on either or both circuits and for these to consequentially fail to reseat. Failure of a relief valve on the primary side to reseat will result in a consequential Loss of Coolant Accident (LOCA).

54 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 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.

55 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.

2.3.2.2.2 ND Assessment

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

- 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;

- feedwater system pipe break.

57 All the above events are considered to be Condition II events, with the exception of a feedwater system pipe break, which Westinghouse considers to be a Condition IV event. I have chosen to sample the last two faults listed above on the grounds that feedwater system piping failure is the most limiting fault according to Westinghouse, and loss of normal feedwater flow is the most bounding of the more frequent faults in terms of the performance of the PRHR.

58 In this preliminary assessment performed for Step 3 of the GDA, only the design basis analyses have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such faults performed to underpin the success criteria for the PRA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

59 The feedwater system piping failure assessment assumes the rupture of a main feed line. Westinghouse is still in the process of producing a Fault Schedule for the AP1000 and so it is not possible to explicitly state what initiating frequency is being assumed for this event but given this is a passive failure the likely frequency would appear to be consistent with the assumption of a Condition IV event that is being made by Westinghouse. 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.

60 Westinghouse has indeed treated the fault as within the design basis and identified what it considers the most onerous single failure (failure of one discharge valve on the PRHR). Clearly, the failure of a PRHR discharge valve to open will reduced the rate the PRHR is able to remove decay 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 failing to reseat on demand as a potential candidate for the single failure. Presumably, Westinghouse regards this as being covered by the Condition II inadvertent opening of a pressuriser safety valve case which is considered in the decrease in reactor coolant inventory fault section of the design basis analysis but this needs to be demonstrated. The assumption made about whether a consequential loss of grid occurs as a result of the reactor trip causing the RCPs to coast down could be potentially significant for these transients as the RCPs contribute extra heating that is comparable to the level of decay heating. However, tripping the RCPs results in natural circulation cooling which causes a reduction in the removal of heat from the core. This increases the average core temperature. Comparison of the faults analysed in this section of the DCD suggests that the two effects largely cancel out for these transients although no sensitivity studies are provided to demonstrate that this is the case.

61 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 which has a number of non-redundant valves on the system. Westinghouse argues that all of the non-redundant valves on the PRHR system will be left in the open position during normal operation apart from the PRHR discharge valves which have redundancy and which are tested on a regular basis. However, there is no way of testing whether the non-redundant valves are open once the reactor is at power. Westinghouse is arguing that failure of these non redundant valves represents a passive failure. Such failures do not need to be considered within the US definition of the single failure criterion for a period of up to 24 hours following an initiating event. Westinghouse uses the definition of the single failure criterion defined in SECY 77 439 (Ref. 16) which dates from 1977. In the UK, passive failures are considered within the single failure criterion (Ref. 13). They were also considered as part of the Sizewell B design, which represents relevant good practice for PWR technology in the UK.

Furthermore, in the UK, failure of a non-return valve to open on demand or a steam isolation valve to close on demand is considered to be an active and not a passive failure. For this reason, I am raising a generic RO requiring 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. Should any such single failures be identified there will be a need for an As Low As Reasonably Practicable (ALARP) assessment to see if the design can be changed to eliminate the single failure.

62 It should be recognised that since the construction of Sizewell B, the single failure criterion in SAP EDR.4 has been changed in that the single failure applies only to the safety function and not to a safety system. In the particular instance of the PRHR, it may well be possible for Westinghouse to argue that the PRHR meets the single failure criterion since the safety function to which it is contributing is the removal of decay heat and this can also be met through the actuation of the Automatic Depressurisation System (ADS) allowing cooling from the Passive Core Cooling System (PXS). These safety systems are claimed to be diverse from the PRHR and have been qualified using design basis methods. Furthermore, 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 has only been qualified for operation under natural circulation conditions when the pressure of the primary circuit is above the set pressure of the accumulators.

63 An important characteristic of the AP1000 design is that the ADS in conjunction with the PXS effectively 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. If Westinghouse can demonstrate during Step 4 that there are no detrimental safety issues associated with automatic depressurisation, then this feature appears to be a significant safety improvement on the previous generation of PWR designs, meeting, for example, the requirements of SAP ESS.8 by eliminating the need for operator action.

64 From a systems perspective, the AP1000 has the potential to claim three diverse heat removal systems; the start-up feedwater system which provides feed to the two steam generators, natural circulation cooling from the single PRHR, and cooling using the ADS and PXS which is provided with redundancy. This is only a possibility at the moment because currently Westinghouse is not proposing to qualify the start-up feedwater system to safety system standards and so it cannot be claimed as a safety system. Sizewell B also has three diverse feed systems, redundant motor driven feed to the steam generators, redundant steam turbine driven feed to the steam generators, and bleed and feed using the safety injection system and which is also provided with redundancy but requires manual operation. Importantly, all these systems on Sizewell B are qualified to safety system standards.

65 Most safety systems on Sizewell B are also provided with four-fold redundancy. The design basis assumption (Ref. 13) 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 maintenance on a safety system is forbidden by the technical specifications, the requirement for a safety system to have four redundant trains can immediately be relaxed to three. Westinghouse could claim 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 steam generators and the one PRHR, if the start-up feedwater system were to be qualified to safety system standard. In my judgement, this would meet the single failure requirements of SAPs FA.6, EDR.2 and EDR.4 and possibly exceed them given that one of the trains (the PRHR) is a diverse design to the other two trains (the SGs).

Westinghouse's design philosophy on AP1000 is to simplify the system design as much as possible. I agree with Westinghouse's concept, providing that where additional diversity is being provided by two safety systems (compensating for the reduction in redundancy on a single safety system), both these systems are qualified to an appropriate safety system standard.

66 In Fig 15.2.8-5 of the DCD, the pressuriser pressure transient as calculated by Westinghouse using the LOFTRAN computer code 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 SG water level.

67 The pressuriser water volume transient for the feedline break fault is presented in Fig 15.2.8-6 of the DCD. 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 water level and so it is crucial that the estimated natural circulation flow and heat removal capability of the PRHR is correctly estimated. The validation evidence for the data on the PRHR flow resistances and heat transfer correlations therefore needs to be reviewed in Step 4. However, it should be recognised that claims on natural circulation cooling in PWRs are not novel and the height of the PRHR above the core is comparable with that of the steam generators. In my judgement, a system such as the PRHR could be made to work in principal but the evidence supporting the validation of these claims will need to be reviewed in Step 4 to provide confidence that the system will work as intended when judged against the requirements of the heat transport SAPs EHT.1 to EHT.4 and the validity of assurance SAPs FA.17 to FA.22.

68 Westinghouse concedes that the loss of normal feedwater is 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. There is therefore a need for Westinghouse to consider the following sequence of events that are claimed to protect against a loss of normal feedwater fault and demonstrate either a diverse safety system exists or the inherent characteristics of the plant will provide protection for each of the relevant safety functions:

- fault detection;
- opening of the safety relief valves on the secondary circuit;
- initiation of the PRHR;
- initiation of the CMTs (low cold leg temperature signal);
- isolation of steam systems;
- opening of the safety relief valves on the primary circuit;
- closing of the safety relief valves on the primary and secondary circuits.

69 As an example, Westinghouse needs to consider performing sensitivity studies in which 1) common mode failure of the PRHR is assumed and 2) the common mode failure of the CMTs is assumed. In the case of the CMTs, it is noted that initiation of the CMTs probably makes the transient more onerous since it increases the reactor coolant

inventory for this fault. Hence, it may be possible to demonstrate that a diverse safety system is not required for this function. However, it must be recognised that the CMTs also provide extra boration which helps with long term shutdown requirements. These are specific examples of the more general RO noted above that for all frequent faults there is a need to demonstrate a diverse safety system, qualified to an appropriate standard, for each safety function.

70 The need for diversity extends to support systems. For this frequent fault, the ultimate heat sink is provided by the Passive Containment Cooling System (PCS). Although the ADS together with the PXS provide diversity to the PRHR for the decay heat removal safety function, they rely upon this same heat sink system. Normally, feed to the SGs with steam relief provided by the safety relief valves on the secondary circuit would provide the diverse safety system for this safety function but on AP1000 the intention is not to qualify the start-up feedwater system to safety system standards so there appears to be a short fall in the design concept against SAPs EDR.2 and EDR.3. This issue will need to be explored with Westinghouse during Step 4 as part of the response to the RO on diversity noted above.

71 Within the DCD there appears to be 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 In-containment Refuelling Water Storage Tank (IRWST) to boil. 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. A TQ has been raised with Westinghouse and the response will be reviewed as part of Step 4. Assessment of the validation of such modelling against the validity of assurance SAPs FA.17 to FA.22 will be undertaken in Step 4.

72 The pressuriser water volume transient for loss of normal feedwater is presented in Fig 15.2.7-6. Although Westinghouse accepts that this is a much higher frequency event than the feedline break discussed previously, 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 the pressuriser water level.

73 It is also noticeable that the pressuriser safety relief valves lift during this frequent transient potentially threatening a consequential LOCA should one of the safety relief valves fail to close on demand. Unlike AP1000, Sizewell B is provided with Pilot Operated Safety Relief Valves (POSRVs) as well as a diverse set of spring loaded Pressuriser Safety Relief Valves (PSRV). 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 mechanically actuated POSRVs. This issue will be discussed with Westinghouse during Step 4 but it is understood that the start up feedwater system is capable of providing sufficient feed to the steam generators to avoid the lifting of the PSRVs. As noted above, the start-up feedwater system is currently not qualified to safety system standards and so it cannot be claimed within the design basis assessment. It is noted that the design flow from a single start up feedwater pump to the two steam generators is 118 m^3 / h. This is essentially identical to the minimum auxiliary feedwater flow per pump of 114 m^3 / h when delivering to two steam generators that is provided on Sizewell B although it should be noted that the auxiliary feedwater system is a qualified safety system. The thermal power of the two reactors is identical at 3411 MW so the sizing of the start-up feedwater system appears to be sensible.

74 Within Step 3 no attempt has been made to review the radiological assessment supporting the design basis assessment for these faults although it is known that the assessment has been made against US criteria. As noted above, an RO will be raised requiring that such an assessment is made against the UK requirements given in SAPs FA.3, FA.7 and T.4 for resolution during Step 4 although I judge that this is probably a methodological issue that is unlikely to lead to the need for additional protection measures for these faults.

75 The Westinghouse analysis uses the LOFTRAN computer code to model these heat-up transients. The validation evidence for this code against SAPs FA.17 to FA.22 has not been assessed in Step 3. 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 (see also Section 2.3.2.6). I will review the validation evidence supporting the calculational route during the Step 4 assessment.

76 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 appropriate given 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 x 10^{-2} per demand, there is a case for considering such sequences to be within the design basis according to SAP FA.5 depending upon the frequency of the initiating event. This issue will need to be explored further with Westinghouse during Step 4 of the GDA, once the Fault Schedule is available. Again, there is no discussion of how the reactor will be brought from the controlled state to the safe shutdown state.

2.3.2.3 Decrease in Reactor Coolant System Flow Rate Faults

2.3.2.3.1 Summary of Requesting Party's Safety Case

77 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.

78 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 reactor protection system 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.

2.3.2.3.2 ND Assessment

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

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

80 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 and yet Westinghouse's design rules would allow DNB and limited fuel rod damage to be conceded for this fault.

81 In this preliminary assessment performed for Step 3 of the GDA, only the design basis analyses have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such faults performed to underpin the success criteria for the PRA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

82 This fault considers the loss of reactor coolant flow as a result of the simultaneous coasting down of both RCPs. The fault is treated as a design basis transient and so meets the requirement of SAP FA.5. There is multiple redundancy provided within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met. This transient analysis focuses on demonstrating that the protection system can successfully trip the reactor sufficiently quickly 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, all these parameters can be confirmed during commissioning tests on the reactor prior to operation. There is no discussion about achieving successful post-trip cooling presumably because this is judged to be bounded by other faults. As this is a frequent fault, I would expect the ATWT condition to be presented somewhere within the design basis analyses. This is a generic issue and is discussed in the section on ATWT faults presented below. The present analysis is therefore judged not to meet the requirements of SAPs FA.6 and EDR.2 and EDR.3 on the need for diversity. As noted below, an RO will be raised on the need for a design basis analysis of the ATWT fault.

83 The analysis results for DNB are summarised in Fig 15.3.2-6 which illustrates the DNB ratio as a function of time. The results suggest that there is adequate margin to DNB. However, there is still a need to review the uncertainties that Westinghouse has applied to its DNB correlations against the validity of assurance SAPs FA.17 to FA.22. In particular, this transient is very sensitive to the initial starting conditions of the fault since 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. The treatment of uncertainties for this fault will be reviewed in detail in Step 4.

84 Within Step 3 no attempt has been made to review the radiological assessment supporting the design basis assessment for these faults although it is known that the assessment has been made against US criteria. As noted above, an RO will be raised requiring that such an assessment is made against the UK requirements given in SAPs FA.3, FA.7 and T.4 for resolution during Step 4 although I judge that this is probably a methodological issue that is unlikely to lead to the need for additional protection measures for these faults.

85 The Westinghouse analysis uses the LOFTRAN, FACTRAN and VIPRE-01 computer codes to model these decrease in flow rate transients. The validation evidence for these codes against SAPs FA.17 to FA.22 has not been assessed in Step 3. For the Step 4 assessment, I will review the validation evidence supporting the calculational route.

2.3.2.4 Reactivity and Power Distribution Anomalies

2.3.2.4.1 Summary of Requesting Party's Safety Case

86 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, single RCCA withdrawal, withdrawal of banks of rod control clusters assemblies, or reduction in the degree of boration in the primary circuit.

87 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 reactor protection system is able to detect the fault and trip the reactor sufficiently quickly to either prevent DNB or avoid significant fuel damage.

88 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.

2.3.2.4.2 ND Assessment

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

- 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;
- spectrum of RCCA ejection faults.

90 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. I have chosen to sample three of the above faults. The first fault is the uncontrolled RCCA bank withdrawal at power 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, and the integrity of the fuel due to Pellet-Clad Interaction (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 for this fault. The third fault is the rod ejection fault which Westinghouse judges to be the most bounding fault in terms of fuel damage. The remaining faults will be reviewed as part of the Step 4 review. In particular, 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. 45) in France.

91 In this preliminary assessment performed for Step 3 of the GDA, only the design basis analyses have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such

faults performed to underpin the success criteria for the PRA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

92 The uncontrolled withdrawal of an RCCA bank at power fault is treated as a design basis transient and so meets the requirement of SAP FA.5. Westinghouse claims that there is multiple redundancy within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met. This transient analysis focuses on demonstrating that the protection system can successfully trip the reactor sufficiently quickly 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. There is no discussion about achieving successful post-trip cooling presumably because this is assumed to be bounded by other faults. As this is a frequent fault, I would expect the ATWT condition to be presented somewhere within the design basis analyses. This is a generic issue and is discussed in the section on ATWT faults presented below. The present analysis is therefore judged not to meet the requirements of SAPs FA.6 and EDR.2 and EDR.3 on the need for diversity. As noted below, an RO will be raised on the need for a design basis analysis of the ATWT fault.

93 To aid my judgement of the uncontrolled RCCA bank withdrawal fault, I have benchmarked the analysis approach adopted by Westinghouse against the safety case analysis for Sizewell B (Ref. 17) as an exemplar of relevant good practice in the UK. However, no attempt has been made within Step 3 to make a detailed assessment of the computer codes against the validity of assurance SAPs FA.17 to FA.22. Again, such work will be performed as part of Step 4.

94 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.

95 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.

96 The analysis results 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.

97 Sizewell B has both a primary protection system (PPS) and secondary protection system (SPS) through which the following the 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). It is noticeable 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 the overtemperature ΔT trip on 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 but it does possess in-core detectors. However, these are not connected to the protection system and so cannot trip the reactor automatically. Hence, there is no diversity for high flux reactor trip protection on the AP1000 and so the requirements of SAP ESS.7 are not met. The AP1000 is also not provided with a reactor doubling time trip signal for very low power operation.

98 When the 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 that are claimed were presented. The only reactor trip parameters plotted by Westinghouse on Fig 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. Hence, the requirements of SAPs ESS.2, ESS.4 and ESS.6 have not been met. 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 and so to list them as protection against the fault is misleading. It is clear from the figure 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 and demonstrates that there is always two trip parameters that provide effective protection against DNB for the full range of reactivity insertion speeds.

99 There is no discussion of PCI failures as a result of the reactivity insertion faults within the Westinghouse analysis. As noted in the ND fuel assessment report (Ref. 8), Westinghouse's proposed clad stress limit is not necessarily protective against PCI failures for frequent faults (i.e. for faults with an initiating frequency greater than 1 x 10^{-3} per year). This contrasts with the Sizewell B position (Ref. 18) where this is an accepted design criteria for the fuel. In the case of AP1000, meeting this requirement will prove more challenging because of the higher linear rating of the fuel compared with Sizewell B. It is interesting to note that Sizewell B did consider implementing a Delta-kW / m protection system to protect against PCI failures in frequent fault conditions (Refs 18 and 19) but the system was never implemented because Sizewell B was able to demonstrate sufficient margin with its current protection system.

100 In summary, Westinghouse will need to review this fault condition. They need to demonstrate that diversity of protection against DNB exists for the full range of fault speeds and power levels and that at least a single line of protection is provided against PCI failures. They also need to consider the feasibility of connecting the in-core detectors to the reactor protection system. These issues will be raised as ROs.

101 RCCA misalignment covers a range of faults including:

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

102 I have chosen to sample the withdrawal of a single RCCA fault as this is Condition III event for which Westinghouse concedes that there is a potential for DNB to occur. Although a discussion of the analysis methodology and results is provided within the DCD, 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, 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 DNBR less than the

safety limit at less than 5%. As this is potentially a frequent fault with an initiating frequency that could be greater than 1 x 10^{-3} per year, I do not consider this to represent an acceptable 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. The AP1000 is also provided with in-core detectors which in my judgement could potentially protect against these faults provided they are connected to the protection system. This issue will need to be explored with Westinghouse during Step 4. The issue of ramp and hold faults also needs to be discussed with Westinghouse.

103 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.

104 Westinghouse has treated the fault as an infrequent Condition IV event that is within the design basis. As this is a passive failure, this seems reasonable and in my judgement is likely to meet the requirements of SAP FA.5, although Westinghouse's Fault Schedule has not yet been reviewed. Westinghouse claims that multiple redundancy is provided within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 should be met. The transient analysis aims to demonstrate that the inherent characteristics of the reactor core coupled with the protection system can successfully control the fault sufficiently quickly 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 counter acts the reactivity insertion.

105 To aid my judgement of these faults, I have benchmarked the analysis approach adopted by Westinghouse against the original safety case analysis provided for Sizewell B PCSR (Ref. 17) as an exemplar of relevant good practice in the UK. I have also studied the relevant Westinghouse topic report (Ref. 20). However, no attempt has been made within Step 3 to make a detailed assessment of the computer codes against the validity of assurance SAPs FA.17 to FA.22. Again, such work will be performed as part of Step 4.

106 The analysis results are summarised in Table 15.4-3 of the DCD, which presents a summary of the key physics parameters for the hot full power and hot zero power cases including the predicted maximum rod worth insertion and the maximum fuel enthalpy and the maximum temperatures of the fuel and cladding. It is interesting to compare the results of the Westinghouse analysis with the Sizewell B analysis (Ref. 17) for the hot full power condition. The Sizewell B analysis presents the results of two sets of calculations. The first calculation uses the same analysis methods as Westinghouse and even refers to the same topic report (Ref. 20). The analysis methodology is clearly a very conservative assessment which uses the TWINKLE code to perform a 1-D axial neutron kinetics calculation. The enhancement in the Doppler feedback that is due to the asymmetric post ejection power distribution is evaluated by 3-D calculational methods (Ref. 20) which are then conservatively applied within the 1-D TWINKLE model. The results for Sizewell B and the AP1000 are virtually identical. The peak fuel centre temperatures are 2649ºC and 2688ºC respectively, and the average fuel temperatures and peak fuel enthalpies are identical at 2163ºC and 170 Cal / g respectively. The second calculation reported in the Sizewell B analysis performs an explicit 3-D calculation using TWINKLE. This significantly improves the results. The peak centre fuel temperature reduces to 1799ºC and the fuel enthalpy reduces to less than 140 Cal / g. These results give confidence in the AP1000 analysis suggesting it is conservative, that the rod bank insertion limits for AP1000 are adequate, and that the results are largely governed by the design of the fuel assemblies and not overly sensitive to the operating

conditions of the reactor core. However, it is known (Ref. 8) that the Radial Averaged Peak Fuel Enthalpy (RAPFE) safety limit against which the peak fuel enthalpy is assessed is undergoing revision by Westinghouse and it is likely that fault analysis will need to move to 3-D methods to accommodate the changes. These developments will need to be reviewed in Step 4.

107 Within Step 3 no attempt has been made to review the radiological assessment supporting the design basis assessment for these faults although it is known that the assessment has been made against US criteria. As noted above, an RO will be raised requiring that such an assessment is made against the UK requirements given in SAPs FA.3, FA.7 and T.4 for resolution during Step 4 although I judge that this is probably a methodological issue that is unlikely to lead to the need for additional protection measures for these faults.

108 The Westinghouse analyses use the TWINKLE, ANC, LOFTRAN, FACTRAN, VIPRE 01 and THINC computer codes to model these reactivity and power distribution transients. The validation evidence for these codes against SAPs FA.17 to FA.22 has not been assessed in Step 3. For the Step 4 assessment, I will review the validation evidence supporting the calculational route.

2.3.2.5 Increase in Reactor Coolant Inventory Faults

2.3.2.5.1 Summary of Requesting Party's Safety Case

109 Faults in this category cause an increase in the inventory of the primary circuit causing the pressuriser level to rise; potentially challenging 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 again seriously 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.

110 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, initiate adequate post trip cooling using the PRHR heat exchanger so avoiding overfilling the pressuriser and over pressurising the primary circuit.

111 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 such that the pressuriser never becomes water solid threatening the structural integrity of the primary circuit.

2.3.2.5.2 ND Assessment

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

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

113 These are both Condition II events according to Westinghouse's classification scheme. I have chosen to sample the first fault listed above on the grounds that Westinghouse regards it as the most bounding fault in this fault category and the fault is unique to the AP1000. In addition, together with the heat-up faults considered earlier, it places constraints on the sizing of the PRHR and the CMTs for a given pressuriser size.

114 In this preliminary assessment performed for Step 3 of the GDA only the design basis analyses have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such faults performed to underpin the success criteria for the PRA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

115 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 tank spuriously operating is that operation of both tanks would only occur following a spurious safeguard ("S") signal which would also trip the reactor. Operation of a single tank allows operation at power to continue making the fault more onerous. The evidence supporting this claim, that there are no failure-modes in the protection system which can result in spurious operation of both CMTs at power, will need to be reviewed in Step 4.

116 Westinghouse has identified that 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 SAP FA.5. 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. There is therefore a need for Westinghouse to consider the following sequence of events that are claimed to protect against the inadvertent operation of the CMTs fault and demonstrate either a diverse safety system exists or the inherent characteristics of the plant will provide protection for each of the relevant safety functions:

- fault detection;
- reactor trip;
- initiation of PRHR;
- opening of the safety relief valves on the primary circuit;
- initiation of second CMT (low cold leg temperature signal);
- isolation of steam systems;
- closing of the safety relief valves on the primary circuit.

117 As an example, Westinghouse needs to consider performing a sensitivity study in which common mode failure of the PRHR is assumed. This is a specific example of the more general RO noted above that for all frequent faults there is a need to demonstrate a diverse safety system, qualified to an appropriate standard, for each safety function.

118 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 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.

119 The pressuriser water volume transient for inadvertent operation of the CMTs is presented in Fig 15.5.1-5. 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. This transient, together with those presented for the feed system faults, provide 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. The margin is small and so the validation of this analysis will need to be reviewed in Step 4.

120 Within Step 3, no attempt has been made to review the radiological assessments supporting the design basis assessment. As noted above, an RO will be raised requiring that such an assessment is made against the UK requirements given in SAPs FA.3, FA.7 and T.4 for resolution during Step 4 although I judge that this is probably a methodological issue that is unlikely to lead to the need for additional protection measures for these faults.

121 The Westinghouse analysis uses the LOFTRAN computer code to model the increase in reactor coolant transients, the code having been modified to incorporate modelling of the passive features on the AP1000. The validation evidence for this code against SAPs FA.17 to FA.22 has not been assessed in Step 3. For the Step 4 assessment, I will review the validation evidence supporting the calculational route.

122 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. This is perhaps appropriate given this design transient section is attempting to demonstrate that the sizing requirements for the PRHR are 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 according to SAP FA.5 depending upon the frequency of the initiating event. This issue will need to be explored further with Westinghouse during Step 4 of the GDA, once the Fault Schedule is available. Again, there is no discussion of how the reactor will be brought from the controlled state to the safe shutdown state.

2.3.2.6 Decrease in Reactor Coolant Inventory Faults

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

- SGTR;
- SBLOCA;
- LBLOCA.

124 Breaks in instrument lines that penetrate the containment have not been assessed for Step 3 of the GDA.

2.3.2.6.1 Summary of Requesting Party's Safety Case for SGTR

125 The design basis fault considered in Chapter 15 of the DCD is the complete severance of a single steam generator 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 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 steam generator power-operated relief valves or the safety valves.

126 Westinghouse has stated in the DCD that a complete severance is conservative because the steam generator 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 Specifications, will not be permitted during operation.

127 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 steam generator overfill and maintain 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.

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

129 The sequence of events following a SGTR is described in the DCD for both automatic and operator recovery actions. In the design basis analysis, the reactor is assumed to trip and lose offsite power concurrent with the rupture of the tube. After reactor trip, the secondary side pressure increases rapidly until the steam generator power-operated relief valves (and safety valves if their setpoint 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.

130 Westinghouse has analysed the plant response following a SGTR until primary-to-secondary break flow is terminated with the LOFTTR2 program. 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. 21). Included within the reference are US NRC’s comments and questions on the changes and their reporting in the applicability report. Westinghouse’s formal responses are also recorded. The codes do not have an explicit detailed model of the ADS as Westinghouse only uses the LOFTRAN codes to model non-LOCA faults (and SGTR faults) where the ADS is not claimed as a safety feature,

131 Westinghouse has provided justification for the use of the LOFTRAN code developed for AP600 to perform analysis of the AP1000 (Ref. 22). 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.

132 Two parallel sets of analyses are undertaken (Ref. 23) for the design basis fault with different assumptions, including different single failure considerations. The main calculation, which is also presented in the DCD, aims to maximise the mass of steam released to provide input to a conservative dose calculation for fault. The second calculation, which is not presented in the DCD, makes assumptions that maximise the mass of water retained in the ruptured SG to demonstrate that there is a margin to overfill.

2.3.2.6.2 ND Assessment of SGTR Safety Case

133 The complete severance of a single SG tube has been analysed in line with expectations for design basis analysis and is also considered in the PRA.

134 Only the results of the thermal hydraulic analysis maximising the steam release to atmosphere are presented in the DCD. The assertion that the SGs will not overfill is a significant safety claim and should be similarly presented with supporting arguments and evidence in the PCSR.

135 Neither the design basis analysis nor the PSA consider multiple tube failures. No justification is provided on why multiple tube failures should not be considered within the design basis. Chapter 6 of PRA (Ref. 24) does state that the plant response to a multiple steam generator tube rupture will be substantially the same as (or more favourable than) the response to a single SGTR. It also states that the multiple SGTR initiating event frequency is significantly lower than the initiating event frequency for single SGTR. However, no evidence for either of these assertions has been seen for Step 3 of the GDA assessment and I will be seeking to pursue this further in Step 4.

136 The fault sequences assumed for both the input to the radiological consequences assessment and for demonstration of a margin to overfill are appropriate. Logical assumptions have been made on the performance of equipment qualified to safety system standard (and those that are not) and single failures have been considered in accordance with the single failure criterion. Although the choices of the worst single failure seem sensible, their selection appears to have originated from work pre-dating the AP1000. Technical queries have been submitted in Step 3 to investigate the selections made and this will be pursued further in Step 4, potentially with the assistance of a Technical Support Contractor.

137 The design basis analysis shows that the leak can be adequately terminated with automatic protection systems but the DCD does not consider the actions required to manage a SGTR from leak termination to a safe shutdown state. Similar observations have already been made for increase and decrease in heat removal faults. As part of a response wider RO, Westinghouse will need to consider this period of the assumed SGTR design basis fault sequence, identifying the adequacy and requirements of systems and operators to achieve safe shutdown. It is observed that if the CMTs have injected their borated water during the earlier stages of the fault sequence, there will be no safety systems to counter-act a subsequent reactivity insertion (e.g. unborated secondary side water passing through the ruptured SG tube). It is expected that the response to the RO will demonstrate if this represents an acceptable position.

138 The fault sequence modelled in the design basis analysis assumes that the CMTs remain in recirculatory mode and that the ADS depressurisation valves are not triggered. The CMTs are a novel development for PWRs and it is therefore intended to investigate their

behaviour and performance further in Step 4 via a Technical Support Contractor running a thermal-hydraulic model of the AP1000 using a code independent of that used by Westinghouse. This will include an investigation into how large an escalation from the design basis fault (i.e. a single tube rupture) is required to change the plant response to drain-down mode and ADS initiation.

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

140 While LOFTRAN & 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 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). Westinghouse subsequently performed a detailed assessment of the applicability of AP600 testing to AP1000. 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. The validation evidence for these two codes has not been assessed in Step 3 of the GDA against SAPs FA.17 to FA.22. An intended Step 4 activity is to employ a Technical Support Contractor to review the appropriateness of LOFTRAN / LOFTTR2, comparing the predicted transient response of the plant to that predicted by a modern code, and to consider the adequacy of the verification and validation records.

141 The DCD presents the predicted Total Effective Dose Equivalent (TEDE) to a member of the public at the site boundary for the design basis fault calculated for both an accident initiated iodine spike and a pre-existing iodine spike. For a limiting 2 hour interval, the dose calculated for an accident initiated spike is 11 mSv and for a pre-existing spike the calculated dose is 22 mSv. The acceptability of the off-site radiological doses is a significant claim made in the DCD. While these doses are beneath the USNRC's criteria, they are above the Target 4 Basic Safety Level (BSL) off-site targets for frequent faults (Ref. 5). It is recognised that the doses have been calculated to a prescriptive methodology approved by the US NRC which could be inconsistent with the expectations for a similar calculations in the UK. It is therefore not appropriate to directly compare the doses presented in the DCD with those presented in Target 4 of the SAPs. 7. As previously noted, an RO will be raised requiring radiological assessments to be undertaken to the UK requirements given in SAPs FA.3, FA.7 and T.4 for resolution during Step 4

142 Any assessment of Westinghouse's application of ALARP in the design is limited until appropriate assessments of the radiological consequences have been made. It is recognised that Westinghouse has utilised operational experience to make their design choices of larger SGs, alloy selection etc. Westinghouse has taken steps to limit the frequency and consequences of the fault and have provided automatic protection systems to prevent overfill. The design is therefore likely to be an improvement on Sizewell B which represents relevant good practice in the UK.

2.3.2.6.3 Summary of Requesting Party's Safety Case for SBLOCA

143 A SBLOCA is defined in the DCD 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 (described as an infrequent fault by Westinghouse). Four types of SBLOCA are considered:

- 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.

144 The passive safety features of the AP1000 are claimed to prevent or minimise core uncovery 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 the CVS make-up system (which is not qualified to safety system standard) fails to perform.

145 A reactor trip and the initiation of the PXS are actuated by the pressuriser low-pressure setpoint 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 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.

146 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. 25). Justification has been provided (Ref. 22) for the appropriateness of using the AP600 version of the NOTRUMP code for the AP1000 analysis.

147 Westinghouse states it has considered active single failures of the passive safeguard systems. They have identified that one of the four ADS Stage 4 valves failing to open on demand is the limiting single failure and this has therefore been modelled in the transient analysis that is presented.

148 The analysis presented by Westinghouse shows that for all but the 10 inch cold-leg break fault the core remains covered and therefore there is no core heatup as a result of the transient. 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 exhibits the potential for core dry-out but without the two phase mixture level dropping into the active fuel region. Via an adiabatic heat up calculation with conservative assumptions, Westinghouse has estimated a peak clad temperature of approximately 743°C. The DCD states that this temperature demonstrates a significant margin to the US NRC limit of 1204°C.

149 In addition to being considered as a design basis SBLOCA (to demonstrate the adequacy of the passive safety systems), the inadvertent operation of the ADS valves (along with inadvertent opening of a pressuriser safety valve) has been considered as a separate pre-trip transient fault within Chapter 15 of the DCD. 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. The pressuriser safety valve fault is a classified by Westinghouse as a Condition II event, i.e. a frequent fault.

150 Although ADS Stages 2 and 3 have larger valves, the transient analysis considers ADS Stage 1 valves because they have quicker opening times. Cases with and without loss of off-site power have been considered. The LOFTRAN code has been used to model the plant system transient and the FRACTRAN code is used to calculate the core heat flux using the LOFTRAN output. Finally the VIRPE-01 code is used to calculate the DNBR.

151 Long term analysis of a non-isolable stuck-open ADS valve or pressuriser safety valve is demonstrated by the small break LOCA analysis.

2.3.2.6.4 ND Assessment of SBLOCA Safety Case

152 Westinghouse has undertaken design basis analysis to demonstrate the adequacy of the passive safety systems to deal with SBLOCA (as defined by Westinghouse to be less than 1.0 ft^2), meeting the requirement of SAP FA.4. In addition to the passive design features, it is recognised that the design of the canned RCPs (attached directly to each steam generator channel head), the lack of reactor vessel penetrations below the top of the core like on Sizewell B, and the location of the core low in the vessel help to reduce the likelihood and consequences of a SBLOCA in an AP1000.

153 A range of breach types and sizes have been considered for an at-power reactor, and the expected sequences for the design basis faults have been described in detail in the DCD with supporting transient analysis. It is expected that breaches considered should bound all candidate small breaks but this will be reviewed further in Step 4 against SAP FA.5. All the SBLOCA faults explicitly discussed in the DCD, and any faults bounded by the discussed faults, should appear on the Fault Schedule.

154 All of the faults have been shown to be acceptable against US NRC criteria and limits. Given that fuel uncovery is stated not to occur for all postulated SBLOCA faults, there is no requirement for any discussion on the acceptability of US NRC criteria for a UK context.

155 The design basis analysis assumes the active failure of one of the four ADS Stage 4 valves as a limiting failure. Further work is required to satisfy me that this aspect of the AP1000 design meets the requirements of SAPs FA.6 and EDR.4. In Step 4, Westinghouse will be asked to produce evidence to support the claim that an ADS Stage 4 failure is limiting. In addition, the amount of margin three out of four ADS Stage 4 valves provide for small break faults will be an area for investigation in Step 4 (I have discussed this issue further in Section 2.3.3.2). It is noted that Westinghouse do not consider the failure of one of the two accumulator check valves within the design basis, asserting that this is very improbable given the large pressure difference that would force the valve open. Nevertheless, in the UK, it is good practice to treat the failure of an accumulator non-return valve as a single failure. This was the case for Sizewell B. However, it is understood that only one accumulator is required to provide adequate levels of post-trip cooling following a SBLOCA although this will need to be confirmed with Westinghouse in Step 4. The acceptability of this assumption on check valve failure is also being considered as part of the assessment of LBLOCA below.

156 The design basis analysis also excludes the failure of the non-redundant valves on the PRHR system as credible active failures. Following a LOCA (and subsequent trip), heat is removed from the RCS by natural circulation through the SGs and the PRHR, and via the break itself. However, since the start-up feedwater system is not qualified to safety system standards, it cannot be claimed within the design basis analysis and so the SGs are assumed to dry out. For the smallest breaks very little energy will be removed by the break itself, and so loss of the PRHR could have a significant impact on those SBLOCA faults associated with very small breaks. Westinghouse will need to present in Step 4 further evidence to support the arguments that these valves can be excluded from the single failure criterion or additional transient analysis will be required to demonstrate the

acceptability of the consequences. Qualifying the start-up feedwater system to safety system standards potentially provides an alternative means of meeting the single failure criterion.

157 The radiological consequences of a LBLOCA have been analysed and shown to be acceptable against US NRC dose limits. The consequences analysed for a LBLOCA are significantly worse than those for SBLOCA faults because extensive fuel melting is assumed. As a result, the radiological consequences will bound the small break faults but the frequency of a LBLOCA will be significantly lower than some of the smaller postulated LOCA events therefore the same limits may not be appropriate. Fuel damage is not predicted for any of the small break faults but there is a release of primary circuit water to the containment. SBLOCAs will need to be considered together with other faults in the response to the RO that is to be raised requiring Westinghouse to calculate the radiological consequences for design basis faults using methods and assumptions consistent with relevant UK good practice and to compare the results against the appropriate Target 4 limit.

158 Although NOTRUMP is an old code and no longer represent ‘state-of-the-art’, it has been subject to verification and validation. The code has been reviewed and certified by US NRC, as have been the modifications made to model (AP600) passive systems. Westinghouse has recognised a number of limitations with the NOTRUMP code, and have presented in the DCD sensitivity analysis with NOTRUMP or alternative calculations to address these shortfalls. These limitations of the NOTRUMP code will be pursued further in Step 4 through discussion with Westinghouse. An intended Step 4 activity is to employ a Technical Support Contractor to review the appropriateness of NOTRUMP, comparing the predicted transient response of the plant to that predicted by a modern code, and to consider the adequacy of the verification and validation records against the requirements of SAPs FA.17 to FA.22.

159 It must be remembered that some Condition III events could be classified as frequent events in the traditional UK approach if their initiating frequency is greater than 1 x10^{-3} per year. For all SBLOCA faults that fall into this category, Westinghouse will need to demonstrate that there are two means of achieving each safety function. For example, common mode failure of the CMT discharge valves to open due to a failure of the protection system would require the operator to respond to manually initiate the ADS system since the water levels in the CMTs will not fall in this situation. Westinghouse will need to demonstrate that this provides adequate protection assuming a 30 minute delay for operator action to meet the requirements of SAP ESS.9. Similarly, initiating ADS Stage 4 provides the means of achieving successful long term cooling. The Normal Residual Heat Removal System (RNS) provides a potentially diverse means of achieving this long term decay heat removal function. However, this system is not qualified to safety system standards and requires operator action to align the system. It is understood that the operator only has 15 minutes to perform this action following initiation of Stage 1 of the ADS. This issue will need to be discussed further with Westinghouse once the review of frequent faults is complete as part of Step 4. However, it is likely that there will be a need for an ALARP assessment to explore the feasibility of qualifying the RNS to an appropriate safety system standard and automating the initiation of the system in line with SAP ESS.8. The issue of single failures (including passive failures) following a break on one of the direct vessel injection lines on the one remaining vessel injection line will also need to be explored further in Step 4. For example, it is understood that there are non-redundant valves on the IRWST injection lines that are normally left open but which cannot be tested while the plant is at power.

160 The assessment of the short-term plant behaviour to the inadvertent operation of a pressuriser safety valve and an ADS valve (Condition II and III events respectively) has only shown the adequacy of the overtemperature ΔT reactor protection signal to prevent DNBR even though it is stated that the pressuriser low pressure protection signal is also

capable of tripping the reactor. For frequent faults, I expect to see a demonstration that there are two safety systems provided for each safety function. In Step 4 Westinghouse will be asked to produce additional arguments and / or analysis to show that the DNBR has adequate margin and that the requirements of SAPs ESS.2, ESS.4 and ESS.6 are met. A TQ has been submitted in Step 3 to investigate the assumptions made on valve opening times and this will be pursued further in Step 4.

161 The transient analysis of the 10 inch cold-leg break which results in a portion of the core having the potential to dry out will also need to be discussed further with Westinghouse in Step 4.

162 The failure of small lines carrying primary coolant outside the containment has been considered within the DCD but has not been assessed for Step 3 of the GDA.

2.3.2.6.5 Summary of Requesting Party's Safety Case for LBLOCA

163 The DCD defines a LBLOCA as a major pipe break with a total cross-sectional area equal or greater than 0.09 m^2 (1.0 ft^2). The fault is identified as a Condition IV event.

164 The design of the AP1000 has been developed with the intention of making failure of the main primary circuit pipe work almost incredible. This means that a double-ended guillotine failure of the primary circuit (i.e. 2A LBLOCA) is not considered as a fault within the formal design basis. However, should the fault occur as a low probability event, it has the potential to represent a significant hazard. The fault has therefore been assessed to demonstrate that it cannot make a significant contribution to plant risk, but without consideration of any additional coincidental failure within the safety injection system.

165 The worst case, from the point of view of cooling the fuel, is a complete failure of the cold leg of the circuit pipe work close to the reactor pressure vessel. Analysis of this fault has been presented in the DCD. Margin to clad temperature safety limits has been demonstrated and US NRC precedent has been cited as a basis for avoiding detailed consideration of fuel damage configurations.

166 The largest Condition IV LOCA considered within the design basis is failure of the pressuriser 'surge line'. This leads to a rapid depressurisation of the RCS, but at a slower rate than in the case of the main pipework fracture. Furthermore, given the location of the surge line, the safety injection flow will mostly pass through the core, therefore providing effective cooling. The Westinghouse analysis of this fault has used similar methods to the main pipe break and calculations have demonstrated that significantly lower fuel temperatures would occur than in the case of the cold-leg fault. In the surge line case, no bursting of fuel pin cladding is anticipated.

167 Large loss of coolant accidents also place demands on the integrity of vessel internal components due to the large pressure loads that can occur in the first few tens of milliseconds of the depressurisation. Westinghouse has assessed the impact of pressure forces on primary-circuit components and demonstrated substantial margins to analysis limits for the surge-line failure case. Analysis has not been carried out for the cold-leg fracture fault on the basis that the sequence is outside the formal design basis.

168 In addition to the surge-line fault, the analysis supporting the PSA also includes spurious activation of all four ADS Stage 4 valves. This fault results in a rapid depressurisation from the hot legs and is similar to the surge-line failure, but the path from the core to the break is longer. The analysis demonstrates that even with failure of one of the accumulators to operate, the expected peak clad temperatures will meet fuel temperature limits by a substantial margin. The DCD does not discuss the likelihood of cladding burst.

169 The pressure of steam discharged into the containment building places demands on the containment integrity; requiring analysis of containment peak pressure. The containment

building has been sized to withstand the limiting LBLOCA, assessed on a conservative basis.

2.3.2.6.6 ND Assessment of LBLOCA Safety Case

170 I have assessed the 2A LBLOCA against SAPs FA 15 and 16 which require a demonstration that no sudden escalation in risk occurs for faults excluded from analysis within the design basis and also against SAP KP2 which requires consideration of severe accidents as part of a strategy of defence in depth.

171 In the cases of the LBLOCA within the design basis, a fuller range of fault-analysis SAPs apply including FA 1-18, although consideration of code validation has necessarily been brief and no consideration of how the analysis relates to operational limits and Technical Specifications has been made.

172 Westinghouse has demonstrated the effectiveness of the emergency core cooling system using established codes and methods, notably the WCOBRA / TRAC model for the fuel response (Ref. 26) and the WGOTHIC code (Ref. 27) for the containment. I take significant comfort from the review of the WCOBRA / TRAC method commissioned by US NRC and carried out by Idaho National Laboratories (Ref. 28). The US NRC review concluded that the analysis methods are fit for purpose and include conservatism in the analysis of the extent to which the coolant is predicted to bypass the core and also in the predicted refilling of the vessel. These are important aspects of the calculation and add confidence in the analysis. I note that this analysis method uses essentially the same code as Sizewell B and also that the associated uncertainty analysis follows best practice (as laid down by the US NRC in the guide NUREG-5249).

173 In the event of a large cold-leg break accident while at power, the reactor vessel and pipe work would rapidly empty and emergency core cooling systems are required to refill the vessel before serious fuel damage can occur. The cold-leg break is considered most demanding on safety systems because it can cause loss of the safety injection water either directly to the break or in the form of entrained droplets carried away by steam returning to the vessel from the intact pipe loop. Given the aggravating features of this particular fault, the analysis is considered appropriate to bound the spectrum of conceivable pipe failures (> 1 ft^2) in terms of severity of consequences.

174 Refill of the vessel is provided by two CMTs and the two nitrogen-pressurised accumulators. Both systems require valve operation to be effective, but Westinghouse argues that the pressure difference experienced by the accumulator check valves in the fault would assist them in opening. This may be a reasonable argument and has been accepted by the US NRC. Furthermore, unverified calculations have indicated that a single failure of an accumulator would not necessarily cause cladding temperature limits to be exceeded. This analysis will be reviewed in more detail in Step 4.

175 Inspection of the predicted cladding temperatures suggests to me that the burst of a number of the hottest fuel pins is likely to occur as a result of a combination of high fuel temperatures and the pin internal pressure. This raises the question of whether blockages of the fuel assembly cooling passages would challenge core coolability. There is no reason to believe that this is a significant issue, but the topic merits specific analysis. I intend to review this further during Step 4.

176 After the RCS is fully depressurised, the coolant is replenished by gravity from the IRWST, which in turn receives condensate off the containment walls via a series of gutters, so passive long-term cooling is available within containment. The high rate of heat transfer to the walls of the containment results in high rates of deposition of particulate fission product on the walls. Westinghouse claims that this avoids the need for active measures to removal iodine and particulate fission products from the containment

atmosphere. This is demonstrated based on relatively simple empirical correlations and will be examined further in Step 4.

177 The containment pressure in the 2A LBLOCA is assessed based on conservative modelling of the steam release from the primary circuit using the WGOTHIC code which is an established multi-volume lumped-parameter model. This analysis effectively determines the size of the containment building and will be considered in more detail in Step 4.

178 The ultimate heat sink in the medium term is air flow over the outer surface of the containment shell. For several days after a fault, forced-convection to this flow must be augmented by evaporation of a flow of cooling water over the outer surface. This water falls by diverse routes from a tank on the roof. The arrangements for long term cooling have been examined by the US NRC and increased redundancy and diversity has been provided. This will be examined in more detail in Step 4.

179 In the medium term, plant operator action may be required to redirect the safety injection to ensure a single-phase coolant flow through the core. The timing for this realignment action is similar to that of existing plant. The human-factors analysis of this operation may need to be reviewed in Step 4.

180 The analysis of the integrity of vessel internals has not been presented for the double-ended guillotine break of the main pipework. Analysis has only been included for the limiting design-basis fault and a high-integrity argument has been claimed for the pipework. In the Sizewell B case, the components with least safety margin to integrity limits were the core barrel (which might crack) and the fuel assembly spacer grids (which might undergo some buckling of the spacer grids in assemblies placed at the edge of the core). These components are important, and failure to make a case for components integrity could potentially invalidate claims made in the PRA on the successful mitigation of these fault sequences. However, it may well be possible to make mitigation arguments for these faults on the basis of failure modes and effects. This will be considered further in Step 4.

181 Inadvertent actuation of all four ADS Stage 4 valves is calculated to lead to partial core uncovery and high fuel temperatures, intermediate in severity between the surge-line failure and a cold leg break. Analysis of the likelihood of fuel clad burst has not been presented. This will be considered further in Step 4.

2.3.2.7 Anticipated Transient without Trip

2.3.2.7.1 Summary of Requesting Party’s Safety Case

182 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 of the design basis faults can be expected to occur relatively frequently with initiating event frequencies greater than 1 x 10^{-3} per year. Such faults are therefore known as anticipated transients. Were such a fault occurs without reactor trip, it is described as an Anticipated Transient without Trip (ATWT).

183 Westinghouse does not consider ATWT events to be within the design basis of the AP1000 and so no design basis safety case is presented within Chapter 15 of the DCD although ATWT is addressed in the AP1000 PRA together with other beyond design basis events consistent with the convention in the US.

2.3.2.7.2 ND Assessment

184 In the UK existing relevant good practice is to consider ATWT faults to be within the design basis (Ref. 29) for PWRs. The Westinghouse position is not therefore considered to be acceptable and so an RO will be raised requiring the preparation of an AP1000 design basis safety case for ATWTs. Westinghouse has supplied some preliminary ATWT analysis (Refs 30 to 32) but this starts from the judgement that the loss of feed fault with failure to trip is the bounding fault due to concerns over primary circuit integrity. I expect that all initiating events with a frequency greater than 1 x 10^{-3} per year to be reviewed against all the relevant safety criteria (fuel integrity, primary circuit integrity) noting that such analysis was performed for Sizewell B (Refs 33 and 34).

185 In the case of Sizewell B, the design was 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 reactor coolant pumps will provide adequate protection for such faults given the inherent characteristics of the moderator temperature coefficients on PWRs. It is understood that this claim applies for all fuel cycle conditions including the initial core. This claim will need to be substantiated in response to the RO and included in an update of the PCSR to meet the requirements of SAP ERC.2. Any response to this RO will need to be reviewed in Step 4.

2.3.2.8 Spent Fuel Pool Faults

2.3.2.8.1 Summary of Requesting Party's Safe Case

186 The Spent Fuel Cooling System (SFS) is discussed in Chapter 9 of the DCD. The SFS is designed to remove decay heat generated by stored fuel assemblies from the water. This is done by pumping the heated water from within the fuel pool through a heat exchanger and returning it to the pool. It also has secondary functions of clarification and purification of the water in the spent fuel pool (and associated tanks / cavities) and transferring water between locations during refuelling operations.

187 The only safety-related function of the SFS identified in the DCD is containment isolation. It is not claimed to operate to mitigate design basis events. In the event the SFS is unavailable, the assumption is that the pool water will heat up and ultimately start to boil. Make-up water from sources qualified to safety system standards is used to maintain the water level above the spent fuel assemblies for at least 7 days.

188 The DCD states that the connections from the SFS to the pool are such that leakage from the system will not result in the pool water level falling to unacceptable levels. In the presented loss-of-cooling analysis it is assumed that the SFS suction pipe shears and the pool is initially drained to that level. Leaks from other (lower) connections to the spent fuel pool are not discussed.

189 The SFS has two mechanical trains of equipment. Each train includes one spent fuel pool pump, one spent fuel pool heat exchanger, one spent fuel pool demineraliser and one spent fuel pool filter. The two trains share common discharge and suction headers. During normal operation, one spent fuel pool cooling system train is operating. The other train is available to perform the other functions of the SFS such as water transfers or IRWST purification. During refuelling, both trains are in operation. One is aligned for spent fuel cooling while the other performs various support functions during the refuelling.

190 The 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. The flow path between the spent fuel pool and the RNS is independent of the flow path used for the spent fuel pool cooling by SFS.

191 Westinghouse is proposing that the cooling functions of both the SFS and the RNS will not be qualified to safety system standard. The heat exchangers for both systems

discharge their heat to the Component Cooling Water System (CCW). Active cooling to the pool would therefore be lost if the electrical power and / or the CCW fail. The heat exchangers have been sized to meet criteria identified in the AP1000 Utility Requirements Document (summarised in Ref. 35). Although no safety claim is placed in the DCD on the active cooling, Westinghouse does have analysis which shows that only a single train of either the SFS or the RNS is sufficient to stop the water in pool boiling in all considered fuel loadings. If off-site power is lost, the SFS pumps can be manually loaded on the respective on-site standby diesel generator, although no claim is placed on this.

192 Chapter 9 of the DCD discusses the results of analysis considering a loss of ac power (off-site and both standby diesels) coincident with a seismic event breaking the SFS piping connections to the spent fuel pool. The stated intention is that the AP1000 can mitigate this design basis event using only passive safety features for 72 hours, and can mitigate this event using only on-site features for 7 days. Calculations (Ref. 36) have been undertaken to determine the time to reach saturation conditions in the spent fuel pool, the time to boil off the spent fuel pool inventory and the make-up water down to the top of the stored fuel, the height of water above the spent fuel and the additional make-up water required from sources not qualified to safety system standards to keep the fuel covered for 7 days.

193 In the worst case, fuel boiling is assessed to begin ~1.37 hours after loss of cooling and make-up is required within 40 hours to prevent spent fuel in the racks becoming uncovered. The DCD identifies the following safety systems as being available to provide sources of water: the cask wash-down pit, the fuel transfer canal, and the passive containment cooling water storage tank. Alignment of the cask wash-down pit is accomplished by positioning manual valves located in the Waste Monitor Tank Room B in the Auxiliary Building. Alignment of the PCS water storage tank is accomplished by positioning manual valves located in the mid annulus access and in the PCS Valve Room in the upper shield building. Westinghouse claims that because these alignments are made by positioning manual valves, they are not susceptible to active failures.

194 After 72 hours, make-up water from the passive containment cooling ancillary water storage tank can either be pumped to the passive containment cooling water storage tank and then gravity fed to the spent fuel pool, or water can be pumped directly to the spent fuel pool.

195 The steam from the boiling spent fuel pool is vented to the outside environment through an engineered relief panel. It is claimed that this maintains the fuel handling area at near atmospheric conditions and that the dose resulting from the spent fuel boiling is small (Ref. 37). The equipment on the fuel handling area (and other areas exposed to elevated temperatures and humidity conditions) is not claimed to provide any mitigation for the fault.

196 The SFS is designed to overflow into the Cask Wash-down Pit and Cask Loading Pit. 54,000 gallons (approximately 200 m^3) of make-up water would be required to overflow the pool onto the operating deck. There are high spent fuel pool level alarms to warn the operator to terminate make-up and the operating deck is equipped with drains to the liquid radwaste system.

197 The spent fuel racks are arranged in two regions. In one region, fresh fuel or any discharged fuel assembly can be placed. In the second region, only discharged fuel assemblies which meet a burn-up versus initial enrichment storage curve can be placed. The racks contain Metamic, a metal matrix composite including boron carbide. The design of the racks is such that the K_{eff} remains less than or equal to 0.95 under design basis conditions, including fuel handling accidents. The DCD states that realistic initial conditions, including boron in the pool water, are assumed in the analysis to demonstrate this. The criticality evaluation uses soluble boron in the spent fuel pool, plutonium decay

time, integral fuel burnable absorber and assembly burn-up as reactivity credit. If flooded with unborated water, the design criterion is that the K_{eff} must remain below 1.0. Analysis showing that this achieved is given in Ref. 38.

198 An assessment of the contribution the spent fuel pool makes to the fuel damage frequency has been done via PRA (Ref. 39). It considers loss of main spent fuel cooling (including loss of CCW), loss of off-site power, loss of all ac power and a safe shutdown earthquake. Fuel damage is assumed to occur at the inception of spent fuel pool boiling with no credit taken for the resumption of SFS or make-up water. The most significant contribution towards the fuel damage frequency is identified as being from the loss of CCW.

2.3.2.8.2 ND Assessment

199 No design basis analysis is presented in Chapter 15 of the DCD for spent fuel pool faults. There is brief consideration given to spent fuel cask drop accidents and 'design basis' fuel handling accidents (dropping of a spent fuel assembly such that every rod on the dropped assembly has its cladding breached). No spent fuel cask operations are anticipated in the early years of reactor operation and therefore it has not been considered a priority for GDA assessment. For the design basis fuel accident, a conservative assessment of the off-site dose has been calculated. A 52 mSv TEDE at the site boundary is compared against a US NRC limit of 250 mSv. Claiming the calculated dose to be well within the limit, the consequences of the fault are claimed to be acceptable. These doses will need to be recalculated using a methodology appropriate for the UK and compared with Target 4 values in the SAPs.

200 The design of the spent fuel pool is functionally similar to existing PWRs, including Sizewell B. Westinghouse has aimed to simplify the design by using fewer components, provide redundancy for more probable failures (although these have not been explicitly discussed in the DCD) and has attempted to use proven components and designs. The significant departure from existing approaches is to make no safety claim on the cooling in favour of letting the pool boil and provide make-up water from safety grade sources.

201 The only pipe break conceded is on the SFS suction pipe. The assumption that the water level falls immediately to this level in the design basis loss-of-power fault is pessimistic. However no arguments have been found in the DCD stating why failures of other (lower) pipes are incredible or why the consequences of such pipe breaks would be acceptable.

202 Loss of cooling faults and pipe leak faults need to be identified systematically on the Fault Schedule, with appropriate supporting design basis analysis to allow assessment against SAPs FA.4 to FA.9. If certain faults do not need design basis analysis because e.g. a leak from a particular pipe is incredible, this needs to be clearly justified. The frequency of a particular fault on the Fault Schedule and the assessed unmitigated consequences should drive the design and classification of protective systems. I intend to raise an RO for Westinghouse capturing this requirement.

203 The adequacy of the active cooling trains to prevent the pool from boiling has been demonstrated (Ref. 35) for events other than loss of power and / or CCW. It is not claimed in the DCD. It is anticipated that this analysis could be usefully utilised in systematic design basis analysis of credible faults providing these systems are qualified to safety system standard.

204 The claim that the dose released from a boiling pool is small is still being investigated. The available supporting arguments and evidence will be reviewed in Step 4.

205 There is no discussion in the DCD of the consequences of the considered loss of power fault occurring while a fuel assembly is being moved above the racks. TQs have been submitted in Step 3 to question this and it will be pursued further in Step 4.

206 There is a reliance on operators responding to alarms and opening manual valves. In the design basis event, the operator will be attempting to open manual valves during a station blackout. In the worst case, boiling would begin in ~1.4 hours. If all the fuel is in the racks, the operator has to provide the make-up water within 40 hours to avoid spent fuel becoming uncovered. However, it is not clear in the DCD how long it would take for stranded in-transit fuel to become uncovered, or if a safety claim is placed on an operator and fuel handing equipment that has not been qualified to safety system standards (in elevated temperatures and humidity) to return the fuel to the racks before it can be uncovered. Again TQs have been submitted to explore this part of the safety case further.

207 The GDA assessment of faults in the spent fuel pool can only be limited until a Fault Schedule has been developed and the safety classification of spent pool fuel structures, systems and components has been revised in line with UK and international good practice. In the DCD, there are no claims placed on the cooling functions of the SFS and RNS. This could change during Step 4 following the work mentioned above. Where claims have been made in the DCD, there is little supporting arguments and evidence. When Westinghouse provides this information in response to the planned RO, it will be requested and reviewed in Step 4.

208 The PRA fuel damage frequency assessment (Ref. 39) makes assumptions consistent with those presented in Chapter 9 of the DCD and therefore does not address the assessment comments made above. It is noted that a low fuel damage frequency (1.59×10^{-10} events per year) is predicted even with the pessimistic assumption that fuel damage occurs on commencement of boiling. No benefit is therefore being taken from the safety grade make-up water to prevent the uncovery of fuel in the racks. On the other hand, the SFS which is not qualified to safety system standards would appear to be making a large contribution to nuclear safety. I intend to investigate the contents of the assessment (Ref. 39) further during Step 4 in cooperation with ND's PSA inspectors.

209 Other ND inspectors will take the lead in assessing the design of the spent fuel racks and the criticality evaluation but the case made for these aspects will be looked at from a Fault Studies perspective in Step 4. In particular, a 'burn-up credit' safety case for the storage of spent fuel, which relies upon administrative controls and operational assessments, will need to be reviewed carefully, cognisant of regulatory views formed during the on-going work to introduce a similar case at Sizewell B. In particular, strong arguments will be needed to justify why it is not reasonably practicable to enlarge the spent fuel pool to eliminate by design the risk of a criticality fault without the need for administrative controls as would be required by a safety case based upon burn-up credit arguments. This would better meet requirements of the hierarchy of safety measures outlined in SAP EKP.5. It is also observed that Sizewell B applies a K_{eff} limit of 0.98 for fault scenarios while the AP1000 assumes a limit of 1.0 for fault scenarios with unborated water. This apparent disparity will be explored further in Step 4, especially given that the AP1000 design makes significant claims on the provision of make-up water from unborated sources.

210 While the AP1000 reactor design contains many novel safety features, the spent fuel pool is very similar in design to existing PWR pools. Given that existing spent fuel pools do not allow the water to boil, Westinghouse needs to make a strong ALARP case stating why allowing boiling represents good practice for a new facility and / or why the difficulties of placing safety claims on the SFS is disproportionate to the benefits it would bring.

2.3.2.9 Shutdown Faults

2.3.2.9.1 Summary of Requesting Party's Safety Case

211 With the exception of CVS malfunction leading to a decrease in boron concentration, shutdown reactor faults are not considered in Chapter 15 of the DCD. Following a review of shutdown risk (Ref. 40), US NRC requested that Westinghouse performs 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 systems, structures and components that are important in maintaining a low shutdown risk for AP600 are generally the same design and / or have the same design basis with respect to their role in reducing shutdown risk. 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 DCD. Despite Chapter 19 of the DCD being nominally about PRA, Appendix 19E includes design basis evaluations of events that can occur during shutdown.

212 Like other PWRs, the operation of AP1000 is characterised by a number (six) of modes. 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.

213 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 while the reactor vessel upper internals are 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 reduces the challenges to the low temperature overpressure events.
- 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.

214 During RCS maintenance, the most limiting shutdown condition anticipated by Westinghouse is with the reactor coolant level reduced to the hot-leg (mid-loop) level and the RCS pressure boundary opened. In this situation, the RNS is used to cool the RCS.

As the RNS is not qualified to safety system standards, its failure has been considered as a design basis fault. In this situation, core cooling is provided by the PXS, using gravity injection from the IRWST, while venting through the ADS valves. The DCD points out that with the RCS depressurised and the pressure boundary opened, the PRHR heat exchanger is unable to remove the decay heat because the RCS cannot heat sufficiently above the IRWST temperature.

215 The IRWST injection squib valves and ADS Stage 4 valves are automatically opened if the RCS hot-leg level indication decreases below a low setpoint (in the considered scenario, the CMTs are isolated and ADS first, second and third stage valves are already open). A time delay is provided to allow time for the operators to restore decay heat removal using systems not qualified to safety system standards prior to actuating the PXS. The time delay with an alarm in the containment serves to protect maintenance personnel. Once the IRWST injection valves and ADS Stage 4 valves open, the IRWST provides gravity-driven injection to cool the core. Containment recirculation flow would be automatically initiated when the IRWST level dropped to a low level to provide long-term core cooling.

216 Each of the design basis accidents and transients considered in Chapter 15 of the DCD are 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 faults are 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 accumulators are isolated. In addition to the at-power faults, Appendix 19E identifies two loss of normal residual heat removal system faults (one in Mode 4 with the RCS intact and one in Mode 5 with the RCS open) for analysis.

217 The double-ended cold-leg guillotine break has been analysed using the WCOBRA/TRAC computer code. The analysis calculated a peak clad temperature of 771°C, which is less than the US NRC limit of ~1200°C.

218 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 that a loss of off-site power occurs, resulting in the loss of the RNS cooling and therefore the 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. Assuming just automatic actions 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 setpoint is reached, resulting in a rapid depressurisation of the RCS. When the CMT level reaches the fourth-stage ADS setpoint, two of the four fourth-stage paths open (assuming one path is out of service and another fails as a single active failure). This final ADS stage allows IRWST injection to begin.

219 If the earlier operator actions have been successful for the loss of normal residual heat removal fault in mode 4, then the CMT and PRHR isolation valves would open but ADS actuation would be avoided.

220 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 DCD. The core stack mixture level is shown to be maintained above the elevation of 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.

221 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 not able to provide a secondary heat sink. The CMTs and PRHR are assumed to be out of service in accordance with permissions set out in Technical Specifications. Only two of the four fourth stage ADS paths are assumed to be available

and one of the two IRWST injection paths is assumed to be out of service in accordance with the Technical Specifications.

222 The transient analysis for this fault has assumed a loss of offsite power, resulting in a 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. One of the two available ADS Stage 4 valves is assumed to fail to open as a single active failure. The core stack mixture level is shown to be maintained above the elevation of 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 Direct Vessel Injection DVI nozzle elevation. The DCD 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.

223 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 pressure boundary design limit being violated and that no high energy piping failure with unacceptable consequences is initiated. 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 (see paragraph 212) 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 DCD states that the operator is instructed to actuate the ADS. 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.

2.3.2.9.2 ND Assessment

224 Although shutdown faults have not been considered alongside at-power faults in Chapter 15 of the DCD, they have been systematically considered in Appendix 19E. However, rather than specifically identifying faults that could occur at shutdown, the sensitivity of the at-power transient analysis to shutdown operation has been evaluated. I intend to make a RO for Westinghouse to identify all potential design basis shutdown faults and present them on the Fault Schedule in accordance with SAPs FA.5 and ESS.11. Faults occurring at shutdown have the potential to result in significant off-site release if adequate protection is not provided and so they need to be assessed using design basis techniques. Shutdown faults are expected to contribute a significant portion to the overall reactor risk reinforcing the need for such faults to be treated in a similar way to at-power faults. However, it is acceptable for at-power transient analysis to be used to bound shutdown faults where appropriate.

225 The approach adopted by Westinghouse has identified and considered the obvious shutdown faults which I would expect to see in addition to those presented in Chapter 15 for at-power faults, i.e. LOCA in shutdown modes, boron dilution faults, and loss of decay heat cooling in shutdown modes. During Step 4, I will look to challenge the completeness of the list of initiating events and the supporting transient analysis.

226 During successive shutdown modes, systems and components can and will be taken out of service. It is not clear in Appendix 19E what safety claims are placed on the remaining systems and / or operators. The RO identified above will also require that safety claims made to protect against shutdown faults are clearly identified.

227 It is recognised that Westinghouse has undertaken an assessment of the non-safety defence in depth features to determine the (US) regulatory treatment of non-safety features (Ref. 41). It is understood that this assessment has resulted in some non-safety (US NRC definition of non-safety) systems having some availability controls placed on them for shutdown. This report will be reviewed in Step 4. However, this work is not strictly relevant to the GDA process because of the requirement for Westinghouse to reassess the safety categorisation of safety functions in accordance with the UK SAPs and to identify the safety claims for shutdown faults as discussed above.

228 For the majority of the Chapter 15 faults, arguments are given as to why no additional analysis is needed for shutdown modes beyond that presented for at-power scenarios. While many of the assertions seem logical, I have found little evidence presented to support these arguments. It is not clearly demonstrated with analysis that the assumptions of less severe shutdown transients, when combined with reduced / inhibited safety systems, result in consequences that are bounded by the at-power fault (for examples, see Chapters 19E4.2.1, 19E4.2.2 and 19E4.2.3 of the DCD). It is also important for the transient analysis to demonstrate that adequate timescales exist for any operator actions that are required to protect against the fault.

229 For some shutdown faults, it is argued that Technical Specification requirements prevent safeguard systems being blocked until certain requirements (e.g. boration to shutdown margins, temperature limits) have been met. As a result of these requirements being met, it is argued that the consequences of a fault, despite reduced safety systems, are bounded by the at-power faults. However there is no discussion in Appendix 19E on how design basis analysis of shutdown faults has fed (or will feed) into the writing of AP1000 Technical Specification requirements. Neither is there any discussion of whether the claims that at-power analysis bounds shutdown faults could be undermined if the operator fails to fully comply with a Technical Specification requirement e.g. before isolating a piece of safety equipment.

230 It is not clear from the DCD how (if it all) design basis analysis defines the various AP1000 shutdown modes apart from the demonstration that the upper temperature limit of Mode 4 can be reached using passive safety systems.

231 The DCD demonstrates the acceptability of LOCA faults during shutdown by stating that the peak clad temperature (771°C) calculated for a bounding double-ended is less than the US NRC limit of ~1200°C. However there is no discussion of whether the radiological consequences for the fault are acceptable against the UK numerical targets presented in the SAPs. Similarly, there is no discussion of the acceptability of the radiological consequences for the loss of decay heat cooling faults. As part of the response to the intended RO for shutdown faults to be presented on the Fault Schedule, frequencies should be attributed to individual faults. As part of the response to the RO to recalculate the radiological consequences of design basis faults, shutdown faults should be considered and the results compared to the numerical targets in the SAPs.

232 It is stated in Appendix 19E that the doubled-ended cold-leg LOCA has been analysed with WCOBRA / TRAC. It is not stated what code was used to assess the loss of decay heat cooling faults. The suitability of WCOBRA / TRAC to assess LOCA faults is discussed in Section 2.3.2.6.5. The analysis of the shutdown transients presented Appendix 19E will be reviewed in detail in Step 4.

233 The AP1000 design does include a number of features for shutdown operations, building upon lessons-learned with regard to shutdown safety from operating PWRs. These design features show that Westinghouse has taken steps to ensure that risks from shutdown faults are reduced. The descriptions of these potential improvements should be complemented by a statement from Westinghouse on why the AP1000 design meets the UK's ALARP criteria for shutdown faults and that there are no further design features that could be added practicably to further reduce the risks. In particular, Westinghouse

will need to demonstrate for shutdown faults, just like all other faults, that the protection systems are provided with adequate redundancy and diversity.

2.3.2.10 Internal Hazards

234 Given the time restraints for Step 3 of the GDA, the Fault Studies aspects of the internal hazards safety case have not been sampled at this stage but will be assessed as part of Step 4.

2.3.2.11 External Hazards

235 Given the time restraints for Step 3 of the GDA, the Fault Studies aspects of the external hazards safety case have not been sampled at this stage but will be assessed as part of Step 4.

2.3.3 Severe Accidents

2.3.3.1 Summary of Requesting Party’s Safety Case

236 In support of the PRA, the Modular Accident Analysis Program (MAAP) is used to evaluate severe accident scenarios of risk significance in accordance with a Risk-Oriented Accident Analysis Methodology (ROAAM). The objective of these studies is to show that the AP1000 containment can accommodate the effects of severe accidents for at least the first 24 hours after the onset of core damage.

237 The design of the AP1000 contains a number of passive features that provide defence against severe accidents.

238 In-vessel retention of core debris by external reactor vessel cooling is a key severe accident mitigation attribute of the AP1000 design. The vessel and its insulation systems are designed to promote ex-vessel cooling and to achieve in-vessel melt retention in the unlikely event of failure of normal safety injection. With the reactor vessel intact and debris retained in the lower head, phenomena such as molten corium-concrete interaction and ex-vessel steam explosion are prevented.

239 The ADS is provided to depressurise the reactor primary circuit in the event of a severe accident and hence to enable passive long-term cooling.

240 The accident mitigation system is designed to minimise the risk of hydrogen burn.

241 The provision of enhanced mitigation measures has been considered as part of an ALARP study and the systems provided optimised.

242 The AP1000 PRA assumes that reactor vessel failure always leads to containment failure. However, studies have concluded that prevention of large fission product releases to the environment is not dependent on the integrity of the reactor vessel. If reactor vessel failure occurs, there may be challenges to the containment integrity, but these challenges are highly uncertain and the most likely challenge (containment failure by melt penetration of the cavity base mat) would not occur in the first 24 hours of the accident.

2.3.3.2 ND assessment

243 I have assessed the Severe Accident analysis principally against SAPs FA.15 and FA.16 which require a demonstration that no sudden escalation in risk occurs for faults excluded from assessment within the design basis. The general key principle KP.2 also applies. This requires consideration of severe accidents as part of a strategy of defence in depth.

On a more detailed level, the Fault Studies SAPs FA.1 to FA.3 have also been assessed although I have not considered radiological analysis of severe accidents in Step 3. No attempt has been made within Step 3 to make a detailed assessment of the computer codes against the validity of assurance SAPs FA.17 to FA.22. Again, such work will be performed as part of Step 4.

244 The general aim of severe accident mitigation is to contain debris from a damaged reactor core as far as practicable or at least to delay its release to the environment to allow time to take appropriate action; in short, to prevent a large early release. No easy benchmark for this aspect of the design exists because recent research and development has introduced the possibility of mitigation systems not considered at the time when existing plant were designed.

245 The design of the AP1000 is based on an underlying philosophy of passive accident mitigation measures in accordance with SAP EKP.5. In the case of severe accidents, the approach consists of depressurising the reactor and initiating cooling under gravity from the IRWST. Generally this will result in reflooding the core, but should this fail and the core subsequently melts, there is a facility for flooding the reactor cavity and cooling the external surface of the pressure vessel. Provided that the vessel is sufficiently depressurised, the design intent is to ensure in-vessel melt retention. This strategy aims to retain as far as possible the maximum number of barriers to release of radiation in accordance with SAP EKP.3.

246 The measures taken to mitigate severe accidents introduce novel features to the plant and are discussed by topic below. A significant amount of research has been carried out to support the concepts as required by SAP FA.15. This has been reviewed in some detail by the US NRC, but some issues remain the subject of further work. I expect to see an updated safety case with a more complete reference trail at the next issue of the PCSR.

247 I have not considered the assessment of individual severe accident fault sequences in detail for Step 3 of the GDA, (with the exception of LBLOCA sequences considered in Section 2.3.2.6.6 of this report). These analyses will be sampled during Step 4 based on the conclusions of an initial review of the PRA.

Depressurisation

248 Depressurisation of the AP1000 RCS, in the event of an accident, is generally provided by automatic actuation of the ADS based on low levels of water in the CMTs. However the operator will depressurise manually if high core outlet temperatures are detected.

249 Redundancy and diversity are included within the ADS design in accordance with SAP EDR.2. Each stage includes two redundant parallel valve paths so that, with the exception of common-cause failures, no single failure prevents operation of the ADS stage when it is called upon to actuate. To actuate the ADS manually from the main control room, the operators actuate two separate controls positioned at some distance apart on the main control board. The ADS stages are interlocked to activate in sequence which is consistent with the principle of failure to safety (SAP EDR 1).

250 This system provides a high level of confidence that the RCS will be depressurised to a level likely to relieve the load on the pressure vessel, but full depressurisation to the level required for gravity reflood is assessed as requiring three out of four valves. Westinghouse examined this as a potential improvement in ALARP optioneering (as required by SAP FA.16). However, the enhancement considered was that of increasing the size of the valves (which proved too costly). A potentially cheaper option (which would reduce availability demands) would be to add an extra valve. However, a significant postulated fault is caused by spurious opening of all ADS Stage 4 valves. This results in a LBLOCA. Westinghouse has been able to show with the current design that the fault does not fail fuel, but the margins may not accommodate additional capacity in

the ADS. I intend to review further Westinghouse's optioneering in this area as part of Step 4.

In-vessel Melt Retention

251 During postulated severe accidents, flooding the reactor cavity with water from the in-containment refuelling water storage tank is intended to prevent vessel failure. The water cools the external surface of the vessel and prevents molten debris in the lower head from failing the vessel wall and relocating into containment. This prevents ex-vessel steam explosion and core-concrete interaction, which threaten containment integrity.

252 Ref. 42 concludes that in-vessel fuel-coolant interaction is unlikely to fail the vessel and Ref. 43 concludes that in-vessel retention depends on the heat flux to the outer surface of the vessel remaining below the critical heat flux for maintenance of nucleate boiling on the outer surface of the vessel. This critical heat flux has been characterised experimentally by prototypic experiments and I believe that the principle uncertainty in assessing this measure is found in determining the composition of melt in the vessel lower head. This is dependent on the progression of the fault.

253 Westinghouse's judgement is that the most likely melt configuration is an oxide layer overlaid with a relatively thick metal layer resulting from the melt of structural steel work. The addition of the molten iron increases the depth of the overlying metal layer and correspondingly reduces the peak heat flux at the edge of the vessel. Other experts point out that the heat flux could be increased by zirconium metal reducing the uranium oxide causing part of the metal layer to fall below the oxide. At present, this issue is unresolved and I await further information from Westinghouse. However, I note that in-vessel retention could be a worthwhile mitigation measure for many postulated faults even if it fails for the most demanding transients - provided that the measures have no serious drawbacks. The most obvious potential drawback is a risk of containment failure caused by steam explosions as molten material leaves the vessel.

254 Westinghouse examined the consequence of fuel-coolant interaction following vessel failure for AP600 and concluded that it would not lead to a steam explosion likely to threaten the containment. This analysis is claimed to be equally applicable to AP1000. Westinghouse therefore discounts a large early release of fission products for cases where the vessel pit is flooded. Ref. 44 contains an independent review of uncertainties associated with in-vessel melt retention and ex-vessel steam explosions. The analysis confirms that in-vessel melt is likely to be retained, but does not discount the possibility of failure. It goes on to confirm that the loading figures evaluated for the vessel and pit structures are supported by their modelling, but points out that significant loading on containment structures is predicted and that the calculations are subject to modelling uncertainty.

255 In the PRA, in-vessel retention is claimed, but vessel failure is modelled as a prompt containment failure. I will consider this issue further in Step 4.

Hydrogen Control

256 Hydrogen is controlled by igniters placed in containment to burn the gas before it can reach concentrations that could result in a large accelerating flame front. This system is supplemented by a pair of catalytic combiners designed to remove hydrogen at concentrations below the flammability limit. Attention has been given to minimising the effect of hydrogen released into containment.

257 For the containment volumes participating in the natural circulation, Westinghouse claims that fission products and hydrogen are uniformly mixed on a short timescale relative to the duration of the release. Furthermore, the Stage Four ADS vents from the RCS hot legs to the loop compartments are designed to take much of the hydrogen generated in the core with the flow, controlling the consequences of the release. The loop compartments are shielded from the containment shell and have a constant source of

oxygen from the natural circulation in the containment. Some hydrogen can burn as a diffusion flame in the loop compartments without threatening the containment integrity.

258 The positioning of compartment vents is also such as to minimise the damage from potential diffusion flames and as long as there is cooling on the inner surface of the containment shell, downward wall flows are expected to prevent stagnation under the dome.

259 The assessment of the potential for hydrogen flame acceleration to generate a shock wave is based on experimental data.

260 These measures are appropriate in principle and will be considered further for selected faults in Step 4.

Passive Containment Cooling

261 The PCS water flow is initiated based on high containment pressure or by the automatic depressurisation system. The condensation rate of steam on the containment dome and shell matches the core steaming rate and limits the containment pressure in the medium term (although provision is included for venting the containment as a means of long-term pressure control).

262 In the AP600 design, the required rates of condensation could be achieved by allowing natural convection to ambient air on the outside of the containment shell. In the case of AP1000, this needs to be augmented in the medium term by evaporation of a falling water film. This water is provided by gravity from a tank on the top of the containment via a redundant and diverse system of valves and lines, including a line that can be connected to an outside water source, such as a fire tender.

263 Westinghouse has effectively subjected the system to a PRA-based ALARP review and as a result has added a third path to the drain lines. This has been reviewed by US NRC and I take comfort from its review. The system forms an important part of the accident mitigation measures and I will consider the case in more detail in Step 4.

264 A by-product of the passive cooling design is the removal of iodine and particulate fission products from the containment atmosphere by thermophoresis and diffusiophoresis resulting from heat transfer to the steel walls of the containment. This reduces the potential benefit of containment sprays. In order to meet US regulatory requirements, Westinghouse has performed an ALARP study of potential Severe Accident Mitigation Design Alternatives (Appendix 1B of Ref. 2). This review concluded that the addition of safety grade sprays is not ALARP. As a result, the AP1000 design does have a containment spray system but no safety case claim is made upon it. This will be further reviewed in Step 4.

Documentation

265 On a presentational level, some topics in Chapter 19 of the DCD refer out generally to discussions with the US NRC. These topics should be discussed in full in any future version of the PCSR.

2.3.4 Review of Step 2 Findings

266 The Step 2 Fault Studies assessment (Ref. 6) of the Westinghouse AP1000 PSR identified a number of technical issues which ND would need to be considered further as part of Step 3. The report concluded that there was a need to review the list of initiating events against SAP FA.2, the identification of limits and conditions against SAP FA.9, the severe accident strategy against SAPs FA.15 & FA.16, the validity of the computer codes and data against SAPs FA.18 & FA.19 including the performance of appropriate sensitivity studies against SAP FA.22, and the need for diverse shutdown system against SAP ERC.2. This report provides a preliminary review of all these requirements with the

exception of the requirements to identify the limits and conditions for implementation of the AP1000 technical specifications and the need to validate computer codes. These reviews will be performed as part of Step 4.

2.3.5 Use of Overseas Regulators Information

267 An initial meeting has been held with the US NRC to share assessment findings on the fault analysis aspects AP1000. Further meetings are planned and attempts are also being made to arrange Multi-national Design Evaluation Programme (MDEP) meetings in the fault analysis area for AP1000. In addition, discussions have taken place with the US NRC about the possibility of sharing computer code input decks for the TRACE and MELCOR analysis codes for the purposes of performing confirmatory analysis using technical support contractors.

2.3.6 Related Research

268 ND is a member of the following OECD nuclear safety research projects:

- the ROSA-2 large scale test facility aimed a supporting research of severe accident phenomenon 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, and;
- the Sandia Fuel Project (SFP) looking into the consequences of severe loss of cooling accidents on a PWR spent fuel pools.

269 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 and is also funding the Health and Safety Laboratory (HSL) to perform Computational Fluid Dynamics (CFD) benchmark activities as part of the OECD international standard problem ISP 39 on the distribution of hydrogen in containment following a severe accident.

2.3.7 Regulatory Observations

270 No ROs have been raised to date in the Fault Studies area. However, I consider that following ROs will need to be raised to address the shortfalls identified in this assessment report:

i) There is a need to demonstrate that the list of design basis initiating events is complete and can be reconciled with the list of faults in the PSA.

ii) A review of all design basis initiating events with a frequency of greater than $1x10^{-3}$ per year to demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each safety function. The single failure criterion also needs to be extended to include passive failures.

iii) Undertake a radiological consequence assessment for each design basis fault against Target 4 of the safety assessment principles.

iv) The proposal to use the BEACON reactor physics code to demonstrate on-line compliance with the fuel safety technical specifications will need to show that an independent method exists for the operator to ensure compliance.

v) Demonstrate that the fuel is protected from PCI failure for frequent faults. The feasibility of connecting the in-core detectors to the reactor protection system needs to be considered.

vi) Include ATWT faults within the design basis. An ALARP justification for not installing an emergency boration system will also be required.

vii) For each fault, Westinghouse to provide evidence that the plant can reach a safe shutdown state from a controlled state.

viii)The assessment of large-break loss-of-coolant accidents compares the fuel cladding temperatures expected against safety limits. This analysis should include detailed consideration of the potential for fuel channel blockage caused by features of the transient such as plastic buckling of spacer grids.

ix) Shutdown faults and spent fuel pond faults need to appear on the fault schedule. Fault analysis is required for all initiating faults that are determined to be within the design basis.

271 The status of these proposed ROs has been summarised in Annex 1.

2.3.8 Plans for Step 4

272 The assessment for Step 3 has focused on scope of the fault analysis and the claims and arguments that are made within it. Step 4 will examine the evidence presented to support these claims and arguments. Amongst the more significant tasks to be undertaken in Step 4 are:

- review Westinghouse's Fault Schedule for the AP1000;
- assess the response to the ROs identified above;
- assess the appropriateness and validity of the computer codes used in accordance with SAPs FA.17 to FA.24;
- assess the thermal hydraulic analysis performed in support of the probabilistic safety analysis success criteria in accordance most relevant parts of the PSA SAPs FA.10 to FA.14, and;
- commission Technical Support Contractors to undertake independent confirmatory analysis of selected AP1000 transients.

3 CONCLUSIONS AND RECOMMENDATIONS

273 In general, the range of faults considered within the DCD is less comprehensive than might be desired. Nevertheless, my judgement is that it is adequate to enable a characterisation of the fault conditions on the AP1000 to be made for the purposes of this interim Step 3 report. More comprehensive information will be required within the PCSR to be assessed in Step 4. As an example, judgements regarding the importance of the basic assumptions in fault analyses depend upon sensitivity studies in which input information is varied. While some information of this kind has been made available, more comprehensive sensitivity analyses will eventually be necessary. Furthermore, the design basis analyses are only concerned with single events as initiators of a fault sequence. Attention needs to be paid to complex situations in which a combination of events may initiate a fault sequence.

274 Notwithstanding these reservations regarding the form and completeness of the safety case, there are no fundamental reasons for believing from the Fault Studies perspective that a satisfactory safety case for AP1000 cannot be made if the comments and ROs made in this report are taken into account. However, it must be recognised that some of these concerns may ultimately require changes to the plant design. In my judgement, these changes are largely associated with changes to the reactor protection system, the diverse actuation system, and the qualification of systems to an appropriate safety

system standard. Nevertheless, it is too early to completely rule out changes to plant layout at this preliminary stage of the assessment. In particular, it must be recognised that the internal and external hazard safety cases have yet to be reviewed from the Fault Studies perspective. Specific findings include:

- There is a need to demonstrate that the list of design basis initiating events is complete including faults at shutdown and on the spent fuel pool. The list of design basis initiating faults will need to be reconciled with those of the PSA. A design basis safety case is required for each fault.
- There is a need for Westinghouse to review all design basis initiating events with a frequency of greater than $1x10^{-3}$ per year and demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each safety function. The single failure criterion also needs to be extended to include passive failures.
- A radiological consequence assessment needs to be performed for each design basis fault against Target 4 of the safety assessment principles.
- The proposal to use the BEACON reactor physics code to demonstrate on-line compliance with the fuel safety technical specifications will need to show that an independent method exists for the operator to ensure compliance.
- There is a need to demonstrate that the 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 needs to be considered.
- Anticipated Transient without Trip (ATWT) faults need to be included within the design basis. An ALARP justification for not installing an emergency boration system will also be required.
- For each fault, Westinghouse needs to provide evidence that the plant can reach a safe shutdown state from a controlled state.
- The assessment of large-break loss-of-coolant accidents compares the fuel cladding temperatures expected against safety limits. This analysis needs to include detailed consideration of the potential for fuel channel blockage caused by features of the transient such as plastic buckling of spacer grids.
- Westinghouse has made a case for the retention of core material in the vessel should the core melt in a severe-accident. The modelling of melt progression is currently a controversial area with significant uncertainty. Further examination of this research is required.

275 It is recommended that these findings, which include the proposed ROs identified in Section 2.3.7, are formally raised with Westinghouse for resolution in Step 4. It is also recommended that the plans that are summarised in Section 2.3.8 should be developed further and taken forward into the Step 4 Fault Studies assessment.

4 REFERENCES

1 *AP1000 Pre-construction Safety Report*, UKP-GW-GL-732, Revision 1, Westinghouse Electric Company LLC, March 2009.

2 *AP1000 European Design Control Document*, EPP-GW-GL-731, Westinghouse Electric Company LLC, November 2008.

3 *ND BMS, Assessment Process*, AST/001, Issue 2, HSE, February 2003.

4 *ND BMS, Guide: Assessment Process*, G/AST/001, Issue 2, HSE, February 2003.

5 *Safety Assessment Principles for Nuclear Facilities*, 2006 Edition, Revision 1, HSE, January 2008.

6 *Step 2 Fault Analysis Assessment of the Westinghouse submission for the AP1000*, AR 2007/16, Westinghouse Electric Company LLC, February 2008.

7 *AP1000 Design Acceptance Application*, GW-GL-710, Revision 0, Westinghouse Electric Company LLC, 2007.

8 *Step 3 Fuel Design Assessment of the Westinghouse AP1000*, AR 09/040, HSE, November 2009.

9 *UK AP1000 Probabilistic Risk Assessment*, Appendix A, Thermal Hydraulic Analysis to support success criteria, Westinghouse Electric Company LLC, November 2008.

10 *Nuclear Safety Criteria for the Design of Stationary PWR plants*, American National Standards Institute ANSI N18.2, August 1973.

11 *Nuclear Safety Criteria for the Design of Stationary PWR plants*, American National Standards Institute ANSI / ANS-51.1-1983, April 1983.

12 *Sizewell B Station Safety Report, Chapter 15*, Nuclear Electric, 1992.

13 *Transient Analysis for DBAs in Nuclear Reactors*, T/AST/034, HSE, November 1999.

14 *A preliminary report of further secondary side blow down sensitivity studies for the Sizewell B PWR*, PWR/R 772, NNC Ltd, October 1983.

15 *Sub-channel thermal-hydraulic analysis at AP600 low-flow steam line break conditions*, Nuclear Technology, Volume 112, December 1995.

16 *Single Failure Criterion*, SECY-77-439, August 1977.

17 *Sizewell B RCCA ejection analysis at Hot Full Power End of Cycle conditions*, PWR/R 991, NNC Ltd, March 1987.

18 *Implications of pellet-clad interaction as a potential fuel failure mechanism*, PWR/R 890, NNC Ltd, May 1984.

19 *Feasibility study for a delta-kW/m protection function for Sizewell B*, PWR/R 882, NNC Ltd, June 1984.

20 *An evaluation of the rod ejection accident in Westinghouse Pressurised Water Reactors using spatial kinetics methods*, WCAP-7588, Westinghouse Electric Company LLC, January 1975.

21 *LOFTRAN & LOFTTR2 AP600 Code Applicability Document*, SSAR-GSC-129 Rev 1, WCAP 14234 and 14235, Westinghouse Electric Company LLC.

22 *AP1000 Code Applicability Report*, WCAP-15644-P Revision 2, Westinghouse Electric Company LLC, March 2004.

23 *AP1000 Steam Generator Tube Rupture Analysis*, APP-SSAR-GSC-516, Rev 0, CN-CRA-01-93, Westinghouse Electric Company LLC, May 2002.

24 *UK AP1000 Probabilistic Risk Assessment*, UKP-G W-GL-022 Rev 0, Westinghouse Electric Company LLC.

25 *NOTRUMP Final Validation Report for AP600*, WCAP-14807 Revision 5, Westinghouse Electric Company LLC, August 1998.

26 *WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident*, WCAP-14171 Rev 2, Westinghouse Electric Company LLC, 1998.

27 *WGOTHIC Application to AP600 and AP1000*, WCAP-15846 (Proprietary) and WCAP-15862 (Non-Proprietary), Revision 1, Westinghouse Electric Company LLC, March 2004.

28 *Code Qualification Document for Best Estimate LOCA Analysis*, WCAP-12945-P-A (P), Revision 1, Westinghouse Electric Company LLC, March 1998.

29 *Sizewell B – A review by HM Nuclear Installations Inspectorate of the pre-construction safety report*, HSE, July 1982.

30 *AP1000 Anticipated transient without scram sensitivity study*, APP-GL-GSC-009_0, Westinghouse Electric Company LLC, March 2002.

31 *AP1000 Anticipated transient without scram analysis using LOFTRAN code*, APP-GL-GSC-012, Westinghouse Electric Company LLC, May 2002.

32 *AP1000 Additional information relating to ATWS events*, APP-SSAR-GSC-634, Westinghouse Electric Company LLC, February 2004.

33 *ATWS investigation on the UK PWR assuming an emergency boration system*, PWR/R 438, NNC Ltd, June 1981.

34 *Extension of the ATWT analysis for Sizewell B to consider faults at frequencies below 10^{-1} per year*, PWR/R 708, NNC Ltd, March 1983.

35 *AP1000 SFS Heat Exchanger Sizing Calculation*, APP-SFS-M3C-013 Rev 1, Westinghouse Electric Company LLC.

36 *AP1000 Spent Fuel Pool Heat up, Boil off, and Emergency Make-up on Loss of Cooling*, APP-SFS-M3C-012 Rev 1, Westinghouse Electric Company LLC.

37 *AP1000 Determination of Doses from Boiling Water in the Spent Fuel Pool*, APP-SSAR-GSC-513 Rev 3, CN-CRA-08-5, Westinghouse Electric Company LLC, 2009.

38 *AP1000 Spent Fuel Pool Criticality Analysis*, CN-PCT-06-3 Rev 2, Westinghouse Electric Company LLC, June 2008.

39 *AP1000 PRA Spent Fuel Evaluation*, UKP-GW-GL-743 Rev 0, Westinghouse Electric Company LLC, December 2008.

40 *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States*, NUREG-1449, US Nuclear Regulatory Commission, September 1993.

41 *RTNSS report*, WCAP 15985 Rev 3, Westinghouse Electric Company LLC.

42 *In-Vessel Coolability and Retention of a Core Melt*, DOE/ID-10460, July 1995.

43 *Lower Head Integrity under In-Vessel Steam Explosion Loads*, DOE/ID-10541, June 1996.

44 *Analysis of in-vessel retention and Ex-vessel Fuel-coolant Interaction for AP1000*, ER/NRC 03-202, January 2004.

45 *Refuelling Error on Dampierre Unit-4*, IRS number 7505, International Incident Reporting System (IRS), IAEA, April 2001.

Table 1

Summary of relevant SAPs and the assessment of the AP1000 against them

SAP	Description	Comment
Fault Analysis		
FA.1 to FA.3	General	The accident analyses performed by Westinghouse in Chapter 15 of the DCD are assessed against the general fault analysis SAPs in Section 2.3.2 of this report.
FA.4 to FA.9	Design Basis	The design basis analyses performed by Westinghouse in Chapter 15 of the DCD are assessed against these SAPs in Sections 2.3.2.1 to 2.3.2.11 of this report. The faults considered are cool-down faults, heat-up faults, flow reduction faults, reactivity faults, increase in coolant faults, loss of coolant faults (including SGTR, SBLOCA & LBLOCA), ATWT faults, spent fuel pond faults, and shutdown faults. Internal and external hazards have been excluded from scope of the Step 3 assessment and will be reviewed in Step 4.
FA.10 to FA.14	PSA	The thermal hydraulic analysis supporting the PSA success criteria will be assessed against the relevant parts of these SAPs in Step 4.
FA.15 to FA.16	Severe Accidents	The severe accident analysis performed by Westinghouse in support of the AP1000 is assessed against these SAPs in Section 2.3.3 of this report.
FA.17 to FA.24	Validity of data and models	The validity the computer codes will be assessed against these SAPs in Step 4 and in selected cases independent confirmatory analysis will be commissioned from technical support contractors.
Numerical Targets		
Target 4	Design Basis Fault Sequences	A Regulatory Observation will be raised in Step 4 requiring Westinghouse to perform a radiological assessment of the design basis faults against the numerical target SAP Target 4.
Engineering Principles		
EKP.3 & EKP.5	Key Principles	The severe accident analysis has been assessed against the defence in depth SAP EK.3 and against the ALARP hierarchy identified in SAP EK.5.

SAP	Description	Comment
EDR.2 to EDR.4	Design for Reliability	These SAPs are reviewed as part of the design basis assessment under SAPs FA.4 to FA.9 discussed above. In particular, the redundancy and diversity of the protection provided for each design basis fault are reviewed in the sections listed above.
ESS.2, ESS.4, ESS.6 to ESS.8, & ESS.11	Safety Systems	The reactor protection system is assessed against SAPs ESS.2, 4, 6, 7 in Section 2.3.2.5. SAPs ESS.8 and ESS.11 are discussed in Sections 2.3.2.2 and 2.3.2.9.
ERC.1 to ERC.4	Reactor Core	The nuclear design of the reactor core is assessed against the relevant parts of these SAPs in Section 2.3.1 of this report.
EHT.1 to EHT.4	Heat Transport Systems	The design of the PRHR heat exchanger is assessed against the relevant parts of these SAPs in Section 2.3.2.2 of this report.

Annex 1 – Fault Studies – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Observations				
RO-AP1000-046	13 Nov 2009	There is a need to demonstrate that the list of design basis faults is complete and can be reconciled with the list of faults identified in the Probabilistic Risk Assessment (PRA).	New RO to be raised.	Step 4
RO-AP1000-047	13 Nov 2009	There is a need for Westinghouse to review all design basis initiating events with a frequency of greater than $1x10^{-3}$ per year and demonstrate that two diverse safety systems, qualified to an appropriate standard, are provided for each safety function. The single failure criterion also needs to be extended to include passive failures.	New RO to be raised.	Step 4
RO-AP1000-048	13 Nov 2009	Westinghouse needs to calculate the radiological consequences for design basis faults using methods and assumptions consistent with relevant UK good practice and to compare the results against the appropriate Target 4 limit.	New RO to be raised.	Step 4
RO-AP1000-049	13 Nov 2009	There is a need to demonstrate compliance with the fuel safety technical specifications that is independent of the BEACON code.	New RO to be raised.	Step 4
RO-AP1000-050	13 Nov 2009	There is a need to demonstrate that the fuel is protected against PCI failure for frequent faults. The feasibility of connecting the in-core detectors to the reactor protection system needs to be considered.	New RO to be raised.	Step 4
RO-AP1000-051	13 Nov 2009	ATWT faults need to be included within the design basis. An ALARP justification for not installing an emergency boration system will also be required.	New RO to be raised.	Step 4
RO-AP1000-052	13 Nov 2009	For each fault, Westinghouse needs to provide evidence that the plant can reach a safe shutdown state from a controlled state.	New RO to be raised.	Step 4
RO-AP1000-053	13 Nov 2009	For large-break loss of coolant faults Westinghouse needs to provide evidence that the fault will not result in a loss of coolable geometry	New RO to be raised.	Step 4

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
RO-AP1000-054	13 Nov 2009	Shutdown faults and spent fuel pond faults need to appear on the fault schedule. Fault analysis is required for all initiating faults that are determined to be within the design basis.	New RO to be raised.	Step 4