Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 FAULT STUDIES ASSESSMENT OF THE EDF AND AREVA UK EPR

DIVISION 6 ASSESSMENT REPORT NO. AR 09/028-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 EDF and AREVA Pre-Construction Safety Report (PCSR) 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 Studies 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 examined in detail and in selected cases independent confirmatory analyses will be performed.

I conclude that EDF and AREVA have 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 and can be reconciled with the list of initiating events in the PSA.
- There is a need for EDF and AREVA 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.
- EDF and AREVA will need to describe what are the limits and conditions they are proposing for the fuel safety technical specifications.
- There is a need to demonstrate that the fuel is protected from Pellet-Clad Interaction (PCI) failure for frequent faults.
- The response to loss of coolant accidents is generally to shut down the reactor and initiate a partial cooldown via the secondary side. The rate of cooldown identified for the UK EPR is 250°C/h but the majority of the transient analysis presented has assumed 100°C/h. There is a need for EDF and AREVA to provide more analysis at the planned cooldown rate for the UK EPR to demonstrate the adequacy of medium head safety injection for the relevant range of loss of coolant accidents.
- 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 similar to the one installed on Sizewell B will also be required.
- There is a need for EDF and AREVA to demonstrate their safety case for heterogeneous boron dilution beyond what is discussed in the PCSR.

LIST OF ABBREVIATIONS

ALARP	As Low as Reasonably Practicable
ATWS	Anticipated Transient without Scram
ATWT	Anticipated Transient without Trip
BMS	(Nuclear Directorate) Business Management System
BOC	Beginning of Cycle
CAMP	Code and Maintenance Programme
C&I	Control and Instrumentation
CCWS	Reactor Component Cooling System
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
CHRS	Containment Heat Removal System
CSARP	Cooperative Severe Accident Research Programme
CVCS	Chemical and Volume Control System
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
EBS	Extra Boration System
ECS	Emergency Charging System
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System
EOC	End of Cycle
ESWS	Essential Service Water System
FPPS	Spent Fuel Pool Purification System
FPCS	Spent Fuel Pool Cooling System
GDA	Generic Design Assessment
HHSI	High Head Safety Injection
HSE	The Health and Safety Executive
HSL	Health and Safety Laboratory
IBLOCA	Intermediate Break Loss of Coolant Accident
IRSN	Institute de Radioprotection et de Sûreté Nucléaire
IRWST	In-containment Refuelling Water Storage Tank
LBLOCA	Large Break Loss of Coolant Accident
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident

LIST OF ABBREVIATIONS

LOOP	Loss of Offsite Power
MDEP	Multi-Design Evaluation Project
MHSI	Medium Head Safety Injection
MOX	Mixed Oxide Fuel
MSB	Main Steam Bypass (to Condenser)
MSIV	Main Steam Isolation Valve
MSRT	Main Steam Relief Train
MSSV	Main Steam Safety Valves
ND	The (HSE) Nuclear Directorate
OECD	Organisation for Economic Co-operation and Development
PAS	Process Automation System
PCC	Plant Condition Category
PCI	Pellet-Clad Interaction
PCSR	Pre-Construction Safety Report
PDS	Primary Depressurisation System
POSRV	Pilot Operated Safety Relief Valves
PPS	Primary Protection System
PRT	Pressuriser Relief Tank
PSA	Probabilistic Safety Analysis
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
PSRV	Pressuriser Safety Relief Valves
PSV	Pressuriser Safety Relief Valve
PWR	Pressurised Water Reactor
PZR	Pressuriser
RAPFE	Radial Averaged Peak Fuel Enthalpy
RBWMS	Reactor Boron and Water Makeup System
RCCA	Rod Control Cluster Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RO	Regulatory Observation
RPS	Reactor Protection System
RRC	Risk Reduction Category

LIST OF ABBREVIATIONS

SAP	Safety Assessment Principle
SBLOCA	Small Break Loss of Coolant Accident
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection System
SPS	Secondary Protection System
TQ	Technical Query
UCWS	Ultimate Cooling Water System
US NRC	United States Nuclear Regulatory Commission

TABLE OF CONTENTS

1 INTRODUCTION 1
2 NUCLEAR DIRECTORATE'S ASSESSMENT 1
2.1 Requesting Party's Safety Case 1
2.2 Standards and Criteria 3
2.3 Nuclear Directorate Assessment 3
2.3.1 Nuclear Design of Reactor Core 3
2.3.1.1 Summary of Requesting Party's Safety Case 3
2.3.1.2 ND Assessment 4
2.3.2 Fault Analysis 5
2.3.2.1 Increase in Heat Removal Faults 9
2.3.2.2 Decrease in Heat Removal Faults 13
2.3.2.3 Decrease in Reactor Coolant System Flow Rate Faults 19
2.3.2.4 Reactivity and Power Distribution Anomalies 20
2.3.2.5 Increase in Reactor Coolant Inventory Faults 25
2.3.2.6 Decrease in Reactor Coolant Inventory Faults 26
2.3.2.7 Anticipated Transient without Trip 36
2.3.2.8 Spent Fuel Pool Faults 39
2.3.2.9 Shutdown Faults 42
2.3.2.10 Heterogeneous Boron Dilution Faults 45
2.3.2.11 Internal Hazards 46
2.3.2.12 External Hazards 46
2.3.3 Severe Accidents 46
2.3.3.1 Summary of Requesting Party's Safety Case 46
2.3.3.2 ND Assessment 47
2.3.4 Review of Step 2 Findings 50
2.3.5 Use of Overseas Regulators Information 50
2.3.6 Related Research 50
2.3.7 Regulatory Observations (ROs) 51
2.3.8 Plans for Step 4 51
3 CONCLUSIONS AND RECOMMENDATIONS 51
4 REFERENCES 53

Table 1: Summary of Relevant Safety Assessment Principles and the Assessment of the EPR against them

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

1 INTRODUCTION

1 This report presents the findings of the Fault Studies assessment of the EDF and AREVA UK EPR Pre-Construction Safety Report (PCSR) (Ref. 1) 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. 2) and its associated guidance document G/AST/001 (Ref. 3). 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. 4) have been used as the basis for the assessment of the Fault Studies aspects associated with the UK EPR 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. 5) a high level review of the EDF and AREVA UK EPR Preliminary Safety Report (PSR) (Ref. 6) 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 UK EPR in a more detailed way by examining the claims and arguments made in the preliminary EDF and AREVA PCSR (Ref. 1). 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. My focus has been on the analysis of plant failures leading to the largest hazards / risks and the most limiting faults within the design.

4 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 examine the thermal hydraulic analysis performed in support of the Probabilistic Safety Analysis (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 the GDA Fault Studies review. EDF and AREVA have produced a Fault Schedule for the UK EPR but this has not been reviewed at this time.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

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

7 In order to achieve these objectives, EDF and AREVA claim to have incorporated the following features into the design of the UK EPR:

- The inherent characteristics of the reactor core design, together with the reactor control and protection systems, results in adequate reactivity control even if the highest reactivity worth Rod Cluster Control Assembly (RCCA) is stuck in the fully withdrawn position. The design also provides for inherent stability against radial and axial power oscillations, and for control of axial power oscillations induced by control rod movements.
- The fixed in-core instrumentation provides continuous monitoring of specified core parameters and, together with the reactor protection system and the passive gravity assisted insertion of RCCAs, will ensure prompt reactor shutdown to mitigate design basis accidents.
- The Emergency Feed Water System (EFWS) which provides feedwater to the steam generators is organised into four separate and independent trains, each with its own water tank and pump. These each supply separately one of the four steam generators and offer enhanced resistance to common cause failures including external hazards.
- The emergency core cooling system which combines the functions of safety injection and shutdown cooling is organised into four separate and independent trains. Each train is fitted with an accumulator, a low pressure injection pump, a medium pressure injection pump and heat exchanger with water supplied from the In-containment Refuelling Water Storage Tank (IRWST).
- The cooling to the spent fuel pool is organised into a two loop main cooling system with a separate and independent third cooling system that mitigates the effects of the loss of the two main cooling trains. Provision is also made to prevent and mitigate the effect of accidental draining of the spent fuel pool.
- The containment building is provided with a metal liner to ensure very low leakage rates. The containment building is double walled to allow collection and filtration of any leakage before release to atmosphere. All penetrations emerge into connected buildings so that leakages may be collected and filtered.
- The ultimate heat sink, which is provided by the Essential Service-Water System (ESWS) and Component Cooling Water Systems (CCWS), is organised into four separate and independent trains each fitted with a pump and a heat exchanger. In addition, EDF and AREVA claim that this main system is backed up by a dedicated circuit comprising two trains fed by specific power supplies which enables heat from corium cooling to be removed in severe accident conditions in the event of a total loss of heat sink.
- A system is provided to recover and spread corium resulting from core meltdown and low pressure release from the reactor vessel. The system consists of a channel which directs the gravitational flow of corium into a large spreading chamber whose floor is covered with a layer of sacrificial material over a network of cooling channels that protects the foundation raft. The thickness of the raft has been increased, thereby preventing penetration by corium. The arrival of the melt in the core catcher triggers the opening of devices that initiate the gravity driven flow of water from the IRWST into the spreading compartment.
- The inner containment and its pre-stressing design take into account the effects of pressure and temperature of the different core meltdown scenarios considered. In particular, the effects due to explosions of the maximum quantity of hydrogen produced during such conditions are included.

2.2 Standards and Criteria

8 Judgements have been made against the 2006 HSE SAPs for Nuclear Facilities (Ref. 4). In particular, the fault analysis and design basis accident SAPs (FA.1 to FA.9), the probabilistic safety analysis 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.2, EKP.3, EKP.5, EDR.1 to EDR.4, ESS.1, ESS.2, ESS.7 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4) have been considered. The requesting parties have assessed the safety case against their own design requirements.

2.3 Nuclear Directorate Assessment

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

10 Following on from the discussion of these three specific areas, I have briefly reviewed the Step 2 findings in the fault analysis area, the use of overseas regulators information, relevant research to the Fault Studies assessment of the EPR. I have also summarised the Regulatory Observations (RO) 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

11 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.

12 The nuclear design aspects of the UK EPR core are presented within Section 4.3 of Chapter 4 of the PCSR (Ref. 1). The basis of the EDF and AREVA safety case is to demonstrate that the design of the core meets the following design criteria:

- The core design power distribution limits, related to safety criteria for normal operation and operational transients are met through conservative design and maintained by the action of the control system.
- The fuel will not operate with a power distribution that violates the Departure from Nucleate Boiling (DNB) design basis for normal operational transients and frequent design basis faults including the maximum overpower condition.
- Under abnormal conditions, including the maximum overpower condition, the fuel peak power will not cause melting.
- Fuel management will be such as to produce values of fuel rod powers and burn-up consistent with the assumptions in the fuel rod mechanical integrity analysis.
- The fuel linear power density at the hot spot is not greater than those found to be acceptable within the body of the safety analysis (as given in Table 1 of Chapter 4.3 of the PCSR) under normal operating condition.
- The maximum reactivity insertion rate due to withdrawal of rod cluster assemblies at power or by boron dilution is limited. For normal operation at power the maximum

rate of change of reactivity due to accidental withdrawal of control banks is set such that the peak heat generation rate and the Departure from Nucleate Boiling Ratio (DNBR) do not exceed the limits at overpower conditions.

- The fuel temperature coefficient is negative and the moderator temperature coefficient of reactivity is kept negative from hot zero power to nominal conditions with all the control rods out of the core. The coolant void coefficient is required to be negative for all conditions.
- An adequate shutdown margin and a sub-critical core are required for at-power and shutdown conditions, respectively.
- The control rods can provide the minimum shutdown margin for all design basis events and are capable of making the core sub-critical rapidly enough to prevent fuel damage from exceeding acceptable limits, assuming that the highest worth rod cluster control assembly is postulated to remain untripped in its is fully-out position (stuck out criterion).
- When fuel assemblies are in the pressure vessel and the vessel head is opened or being removed, the core must be maintained sufficiently sub-critical to guarantee the safety of the reactor in case of an accidental transient occurring in this state. The accidental transients considered are boron dilution and removal of all rod cluster control assemblies.
- The plant is inherently stable to power oscillations at the fundamental mode.
- Spatial power oscillations within the core with a constant power output, should they occur, can be reliably and readily detected and suppressed.

2.3.1.2 ND Assessment

13 The design of Pressurised Water Reactor (PWR) reactor cores is a well established technology. The changes made to the UK EPR core when compared with the earlier generation of EDF and AREVA 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 the EDF and AREVA 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. 7) 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.

14 The design intent of the UK EPR core is to reduce the maximum soluble boron concentration in the core at the start of cycle by using burnable poisons co-mixed with the fuel material itself to avoid a positive moderator temperature coefficient at beginning of life. During operation the poison content in these rods is depleted, adding positive reactivity to offset some of the negative reactivity from the fuel depletion and fission product build-up. EDF and AREVA argue that through the use of this measure, the initial soluble boron concentration at the start of the first fuel cycle will be reduced to ensure that the moderator temperature coefficient is always negative for at power conditions. This is an important consideration for fault conditions including, for example, ATWT events. These claims will need to be reviewed in detail in Step 4 against the requirements of SAP ERC.3. 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 coefficient for the full cycle length using burnable poisons will be explored with EDF and AREVA in

Step 4. This is part of a more general finding with the EDF and AREVA submission concerning the need to clearly define the fuel safety limits and conditions.

15 It is noted that EDF and AREVA are also proposing to use B10 enriched boron to reduce the quantities of soluble boron required. The controls that will be in place to ensure sufficient quantities of enriched boron are present in the coolant will also need to be reviewed in Step 4.

16 The design requirement to meet 1) the stuck rod criterion and 2) to ensure the fuel will be maintained sufficiently subcritical such that removal of all RCCAs would not result in criticality would appear to meet the requirements of ERC.1 although there is a need to apply an appropriate uncertainty allowance in such assessments. This issue will be discussed with EDF and AREVA during Step 4 although it is noted that in practice the shutdown margin for the stuck rod criterion is likely to be significantly greater than that for Sizewell B.

17 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 in the X-Y plane, are possible. The size of the UK EPR core is larger than Sizewell B core. In particular, the length of the UK EPR core at 4.27 m (14 ft) is longer than many previous cores, including Sizewell B (3.66 m or 12 ft), and so the reactor will be slightly less stable in the axial direction. Although EDF and AREVA do not discuss this issue, the axial stability index will become zero earlier in the cycle length although they do claim 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 will need to be explored further in Step 4 in order to ensure that the requirements of SAP ERC.3 are met.

18 A related matter is the need for the operator to demonstrate compliance with the fuel safety limits that will be identified in the technical specifications. The technical specifications will in turn need to be derived from the limits and conditions identified in the safety case so as to meet the requirements of SAP FA.9. EDF and AREVA are not proposing to issue draft technical specifications until the GDA process is complete. Nevertheless, there is a need for the fuel safety limits and conditions to be clearly defined with appropriate allowances for uncertainties. This issue will be reviewed further in Step 4. EDF and AREVA will also need to outline their proposals for how continuous compliance with the technical specifications will be demonstrated in practice to ensure that adequate alarms and indications are provided within the control room.

2.3.2 Fault Analysis

19 The design basis accident analyses for the UK EPR are presented within Chapter 14 of PCSR (Ref. 1) with the exception of the overpressure protection design basis analysis which is presented in Chapter 3 and the containment design basis analyses, which are presented in Chapter 6. A summary of the results of the thermal hydraulic analyses that underpin the PSA success criteria is presented in Chapter 15. Fault sequences that EDF and AREVA considered to be risk significant but which are not included within the design basis analysis are reported in the risk reduction analysis of Chapter 16 which also presents the severe accident analysis. Overall, I judge that the extent of analysis largely meets the requirements of SAP FA.1 which requires fault analysis should be carried out comprising design basis analysis, probabilistic safety analysis and severe accident analysis although in some areas, as discussed below, additional analysis will be required.

20 EDF and AREVA have classified all faults into four Plant Condition Categories (PCCs) and two Risk Reduction Categories (RRCs). EDF and AREVA have allocated all the design basis events into the four PCCs according to the anticipated frequency of

occurrence and the potential radiological consequences to the public. The four PCC classes are defined as follows:

- PCC-1: Normal operating transients
- PCC-2: Design basis transients (10^{-2} per year < f)
- PCC-3: Design basis incidents (10^{-4} per year < f < 10^{-2} per year)
- PCC-4: Design basis accidents (10^{-6} per year < f < 10^{-4} per year)

21 The first of the two risk reduction categories is allocated according to its contribution to the Core Damage Frequency (CDF) and the likelihood of early containment failure:

- RRC-A: Risk reduction sequences (10^{-8} per year < CDF < 10^{-7} per year)
- RRC-B: Severe accident sequences

22 Discussion of severe accidents sequences is deferred to the section on severe accident analysis presented below but the RRC-A sequences potentially represent sequences that are traditionally treated as within the design basis in the UK (Ref. 9) and so will be discussed together with the relevant PCC design basis initiating events within this fault analysis section.

23 EDF and AREVA aim to demonstrate that the effective dose to an individual off-site is less than the legal limit for normal operation for PCC-1 and PCC-2 events. PCC-3 and PCC-4 events may result in limited fuel rod failure but should not result in the release of radioactive material above the dose limits specified in the technical guidelines provided by the French nuclear safety authority. These differ from the dose limits and assumptions given in SAPs FA.3, FA.7 and Target 4. A direct comparison with SAP Target 4 is inappropriate at this time until the methodology used by EDF and AREVA can be assessed further.

24 EDF and AREVA identify four types of safety functions in the PCSR; F1A, F1B, F2 and non-classified. An F1A safety function is a function that is required for a PCC event to reach the controlled state. An F1B safety function is a function that is required to reach the safe shutdown state. F2 safety functions are claimed for RRC-A and RRC-B sequences. A system is classified F1A, F1B, F2 or non-classified according to the classification of the highest integrity safety function it must perform. In the design basis analyses of PCC events, F2 and non-classified systems are only considered if they worsen the consequences of the accident. Operator actions are considered but only after 30 minutes if executed from the main control room and 60 minutes if executed locally.

25 The categorisation scheme discussed above appears to be partially based upon the US ANSI / ANS 51.1 1983 standard (Ref. 8) which dates from 1983. It is noticeable that the categorisation scheme only considers single events as initiators of a design basis fault sequence. It does not consider complex situations in which a combination of events may initiate a fault sequence. Section 14.0 of the PCSR confirms that PCC events only contain events caused by the failure of one component, the failure of one control and instrument function, one operator error, or the loss of off-site power. In the UK, it is 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. 9). This is the approach that was adopted for Sizewell B. Given that SAP EDR.3 limits the reliability claim that may be placed on any safety system to be no better than 1 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, qualified to an appropriate standard, is required to be provided for each safety function and the functional capability of the system needs to be demonstrated using design basis analysis techniques with appropriate safety margins included to cover for uncertainties. For this reason, an RO will be raised requiring EDF and AREVA to review all design basis initiating events with a

frequency of greater than 1×10^{-3} per year and to demonstrate that a diverse safety system, qualified to an appropriate standard, is provided for each safety function. This extension to the design basis analysis will need to be included within a revision of the PCSR.

26 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. 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 what is the equivalent of F1A standard 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 CVCS on the UK EPR is qualified to F2 standard and it is not obvious that the Extra Boration System (EBS), which has the capability to inject borated water into the core, will automatically provide this safety function should the CVCS fail to operate. This issue will need to be explored further with EDF and AREVA in Step 4.

27 The single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 warrant discussion because of the design criterion definition used by EDF and AREVA. EDF and AREVA only require passive failures to be considered within the single failure criterion after a period of 24 hours following an initiating event. In practice, this is generally not a very onerous requirement and so consideration of passive failures is effectively removed from the requirements of the single failure criterion. This interpretation of the single failure criterion appears to be based upon the US definition of the single failure criterion as defined in SECY 77 439 (Ref. 10), which dates from 1977.

28 In contrast, in the UK, passive failures are considered within the single failure criterion (Ref. 9). 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 and failure of a steamline isolation valve to close on demand are considered as active and not passive failures. For this reason, I am raising an RO requiring EDF and AREVA to perform a review of each design basis fault on the UK EPR to identify whether there are any passive failures on the safety systems that will prevent a safety function from being performed successfully. Should any single failures be identified there will be a need for an As Low As Reasonably Practicable (ALARP) assessment to be performed to see if the design can be changed to eliminate the single failure. 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 to the safety function and not to an individual safety system.

29 A study of the list of design basis analyses presented in Chapter 14 of the PCSR suggests that the faults can also be divided according to the following fault types:

- reactor trip faults;
- increase in heat removal faults;
- decrease in heat removal faults;
- electrical supply faults;
- decrease in reactor coolant system flow rate faults;
- reactivity and power distribution anomalies;
- increase in reactor coolant inventory faults;

- decrease in reactor coolant inventory faults;
- faults affecting non-core sources of radioactivity;
- shutdown faults.

30 This list of design basis initiating events can be compared with the list of design basis initiating events considered for Sizewell B (Ref. 11):

- reactor trip faults;
- increase in heat removal faults;
- decrease in heat removal faults;
- electrical supply faults;
- decrease in reactor coolant system 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;
- faults affecting non-core sources of radioactivity;
- shutdown faults.

31 It is noticeable that the UK EPR design basis list does not include 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.

32 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 in Chapter 15 of the PCSR, it is claimed that the list of initiating events for the PSA is based upon a failure modes effects analysis of the UK EPR systems. In principle, any initiating event identified in the PSA should be included within (or bounded by) a design basis initiating event unless it is screened out on the basis of low frequency as 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 EDF and AREVA list of design basis initiating events with the EDF and AREVA list of PSA initiating events. An RO will be raised requiring EDF and AREVA to perform such an assessment in support of a future revision of the PCSR. This work will need to provide traceability of how failures in essential support systems including the electrical and Control and Instrumentation (C&I) systems have been included or bounded by the PCC events.

33 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 and risk reduction sequence analysis performed by EDF and AREVA 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 reactor coolant system flow rate;

- reactivity and power distribution anomalies;
- increase in reactor coolant inventory;
- decrease in reactor coolant inventory;
  i) Steam Generator Tube Rupture (SGTR);
  ii) Small Break Loss Of Coolant Accident (SBLOCA);
  iii) Intermediate and Large Break Loss Of Coolant Accident (IBLOCA and LBLOCA) within the design basis;
  iv) double-ended guillotine break of primary coolant main pipework (2A-LBLOCA);
- Anticipated Transient Without Trip (ATWT);
- spent fuel faults;
- shutdown faults;
- heterogeneous boron dilution faults;
- internal faults;
- external faults;

34 No attempt has been made to assess the PSA 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

35 Faults in this category result in a cooldown 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 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 building. Finally, a break in the secondary circuit outside containment has the potential for the largest release of radioactive material from the design basis faults in this cooldown category.

36 The basis of the EDF and AREVA safety case is that they have reviewed a number of postulated events that they consider to be within the design basis of the plant and that could result in an increase in heat removal. For those cases which they consider to be limiting they have performed detailed analyses and demonstrated that even for the most bounding faults the reactor protection system is able to trip the reactor, isolate the affected steam generator to reduce the rate of reactor cooldown to ensure an adequate shutdown margin. It is noted that EDF and AREVA do not take any advantage within the fault analysis for the flow of borated water that would be injected from the Medium Head Safety Injection (MHSI) system.

37 In performing the transient analysis, EDF and AREVA have carried out sensitivity studies on a range of initiating faults including a steam line break occurring either upstream or downstream of the Main Steam Isolation Valves (MSIV), a stuck open valve on either the Main Steam Relief Train (MSRT) system and the Main Steam Safety Valve (MSSV) system. They have also carried out sensitivity studies on a range of assumptions including 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)). They also claim to have modelled the worst single failure in the reactor engineered safety features, which in the case of the most limiting fault considered is that the most reactive RCCA fails to enter the core following reactor trip. On the basis of the analysis presented, EDF and AREVA have concluded that adequate protection from DNB is provided for all the range of faults considered.

2.3.2.1.2 ND Assessment

38 EDF and AREVA have considered the following faults within this category that they consider to be limiting and which are presented within the PCSR:

- 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.

39 All these events are considered to be PCC-2 events within the fault categorisation scheme of EDF and AREVA apart from the inadvertent opening of a steam generator relief or safety valve which is a PCC-3 event and the steam system piping failure which is a PCC-4 event. I have chosen to sample the last three faults listed above on the grounds that the steam system piping failure is the most limiting fault according to EDF and AREVA, while the excessive increase in secondary flow fault and the inadvertent opening of a relief or safety valve fault are judged to be the most bounding of the remaining frequent faults.

40 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 PSA 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 PCSR. This work will be performed as part of Step 4.

41 To aid my judgement I have benchmarked the analysis approach adopted by EDF and AREVA against some scoping analysis performed in support of the original Sizewell B PCSR (Ref. 12) as an exemplar of relevant good practice in the UK. This document helps 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.

42 The steam system piping failure assessment assumes the rupture of a main steam line. EDF and AREVA have classified this as a PCC-4 event which has an initiating frequency between 1×10^{-4} and 1×10^{-6} per year. For Sizewell B (Ref. 12) a main steam line rupture inside containment was assumed at 1×10^{-4} per year while one outside containment was conceded at 1×10^{-3} per year. Such frequencies would be consistent with the assumption of a PCC-3 or PCC-4 event. 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.

43 EDF and AREVA have treated the fault as being within the design basis. However, in the case of a steam line break upstream of MSIV, the single failure they choose to consider is failure of the most reactive RCCA to enter the core following reactor trip. The assumption of a stuck out rod is one of the standard deterministic assumptions made within the transient analysis studies of cooldown faults such as those considered here. It is a major factor in determining the shutdown margin of the reactor and whether the core returns to criticality following reactor trip. Making this assumption helps ensure that the overall assessment is conservative, consistent with the requirements of design basis analysis. It is not normal practice in the UK (Ref. 12) to consider this assumption to count as the single failure for the fault. Instead, an additional single failure is normally included within the analysis. 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 a MSIV), the next most onerous failure is probably a failure of one of the MHSI pumps to operate on demand since it is understood that the protection signals that are claimed are all based upon 2-out-of-4 voting logic. EDF and AREVA do not model this single failure but they do make the conservative assumption that the water injected from the MHSI is unborated such that the MHSI contributes to the cooldown of the circuit, through the injection of cold water, but does not increase the boron concentration as would be the case in reality (i.e. the MHSI is assumed to have an effect opposite to one of its designed safety functions).

44 No sensitivity studies to break size and power level are presented within the PCSR. However, the Sizewell B report (Ref. 12) 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 UK EPR at 0.13 m^2, I judge that these results will give an indication of the sensitivity to these parameters for the UK EPR. 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 DNBR with reactor trip occurring on low steam line pressure. For smaller break sizes, including stuck open safety valves 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 EDF and AREVA analyses, which assume that starting at zero power is bounding for both the main steam line break fault and the stuck open / spuriously opened valve on the MSRT or MSSV systems. This may be because the flow capacities of the valves in the MSSV and MSRT systems are much greater than the equivalent valves on Sizewell B such that the balance between tripping on low steam line pressure and low DNBR is altered but EDF and AREVA should be requested to produce further sensitivity studies to confirm the conclusions of their analysis in Step 4.

45 The results of the EDF and AREVA analyses for the steam line break upstream of the MSIV are summarised in Fig. 5 of Section 14.5.2 of the PCSR which presents the return to power transient as a function of time. The power peaks at about 350 seconds at about 17.3%. However, the flux peaking factor associated with the worst RCCA being stuck out is not given. The case assumes that the RCPs are not tripped. EDF and AREVA claim that sensitivities performed in Appendix 14B of the PCSR for the 4900 MWth reactor design demonstrate that the minimum DNBR is not significantly affected by the assumption of RCP tripping at the peak power. After the affected steam generator has emptied, the reactor power stabilises at a power of about 3% which corresponds to the steam discharge associated with the flow from the EFWS to the affected steam generator. The operator is assumed to isolate the EFWS to the affected steam generator after 30 minutes and commence boron injection using the EBS. This causes the reactor to shutdown.

46 EDF and AREVA calculate the minimum DNBR to be 1.42 at about 255 seconds using their own FC CHF critical heat flux correlation (Ref. 1). This meets the requirements of the design basis DNBR limit of 1.12 which they assume for the low pressure conditions that are associated with cooldown faults. These values are low when compared with the design basis value of 2.0 that it is applied at Sizewell B (Ref. 13) 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. It is also noticeable that the DNBR predictions for the sensitivity studies looking into the effect of RCP tripping on the 4900 MWth reactor design were 2.1 and 2.2 for the with and without RCP trip cases respectively. These values are significantly different from those predicted for the final base case and suggest that different analysis methods and techniques were used for the sensitivity studies. This raises questions about the validity of using these sensitivity studies for justifying the assumptions on RCP tripping in the final case. These issues will need to be explored further with EDF and AREVA during Step 4.

47 The results of the EDF and AREVA analyses can be compared with the Sizewell B analyses (Ref. 12) which predicts a 14% peak return to power and a minimum DNBR of 2.27. These results are slightly surprising since the UK EPR is known to possess a much larger shutdown margin than Sizewell B. Although the UK EPR reactor core is larger than the Sizewell B reactor core, it contains proportionality more 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. 12) while the minimum shutdown limit for the UK EPR appears to be 2.7 Niles according to Section 2.1.4.5.1 of the PCSR. The reason why the UK EPR appears worst may be associated with the modelling assumptions for the safety injection systems. As noted above, for the UK EPR, it is assumed that the water that is injected from the MHSI system is unborated. This maximises the cooldown and minimises the shutdown margin. In the case of the Sizewell B analyses, the High Head Safety Injection (HHSI) system is assumed to inject borated water into the reactor helping to shut the reactor down. This assumption of unborated water being injected by the MHSI is somewhat arbitrary and does not give a realistic appreciation of the capability of the MHSI for protecting against this fault. It may well be that the claim on operator action after 30 minutes to initiate EBS flow might be unnecessary if the MHSI, which is qualified to safety system standards, was more realistically modelled assuming only the loss of a single train to take account of the single failure criterion. It is undesirable to claim operator action for design basis faults, as indicated by SAP ESS.8, and so EDF and AREVA will be requested to perform additional sensitivity studies for this fault in Step 4.

48 EDF and AREVA have identified that a stuck open relief or safety valve following a normal operational transient is a PCC-2 event while a spuriously operation of these valves is a PCC-3 event. Given that a PCC-3 can be as frequent as 1×10^{-2} per year, such events must be considered to be frequent events within the traditional UK approach to design basis analysis, which requires two diverse safety systems, qualified to an appropriate standard, to be provided for each safety function to ensure that a design basis sequence frequency of less than 1×10^{-7} per year (Ref. 9) is achieved for an individual fault given the requirements of SAPs EDR.2 and EDR.3 for the consideration of common mode failure. EDF and AREVA do not consider common mode failure of a whole system in coincidence with an initiating event to be within their design basis although they do require that the single failure criterion is met.

49 There is a need therefore for EDF and AREVA 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 or the inherent characteristics of the plant will provide protection for each of the relevant safety functions:

- fault detection;

- reactor trip (if required);
- isolation of the faulty MSSV or MSRT valve;
- isolation of main feedwater and steam systems if required;
- initiation of the MHSI if required;
- initiation of the EFWS if required.

50 As an example, EDF and AREVA need to consider a sensitivity study in which common mode failure of the safety injection system resulting in a failure to inject borated water into the reactor is assumed in coincidence with the worst stuck out rod and then demonstrate, that in the case of cooldown faults, the fuel does not enter DNB. It should be noted that Sizewell B (Ref. 12) 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. 12) also performs sensitivity studies to the case of two stuck RCCAs for the more frequent cooldown faults on the basis that the conditional probability for this event could not be excluded from the design basis sequence requirement of 1×10^{-7} per year (Ref. 9).

51 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 the French safety authority requirements. Such an assessment will be required in Step 4 against the UK requirements given in SAPs FA.3, FA.7 and Target 4. However, I judge that any differences are likely to be minor due to methodological assumptions and it is unlikely to require additional protection measures for these faults.

52 The EDF and AREVA analysis uses the MANTA computer code to model the system transient while the SMART and FLICA III computer codes have been used for the neutronic and thermal hydraulic analysis to determine the whether DNB occurs. The validation evidence for these codes has not been assessed in Step 3 of the GDA against SAPs FA.17 to FA.22 although 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.

53 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 probability for consequential SGTR is as high as 1×10^{-1} per demand. If such high failure on demand probabilities are reflected within UK EPR 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 EDF and AREVA during Step 4 of the GDA.

2.3.2.2 Decrease in Heat Removal Faults

2.3.2.2.1 Summary of Requesting Party's Safety Case

54 Maintenance of design conditions in the reactor depends among other things on preserving, within limits, continuity of heat flow from the reactor through the primary and 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 potentially challenging the integrity of the fuel cladding and causing 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. Faults in this category effectively determine the sizing requirements for the EFWS. They also place the greatest demands on the reliability of the primary and secondary circuit over-pressure protection systems. 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).

55 The basis of EDF and AREVA safety case is that they have reviewed a number of postulated events that they consider to be within the design basis of the plant and that could result in a decrease in heat removal. For those cases which they consider to be limiting, they have 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 EFWS and MSRT system. They also conclude that the MSSV provide adequate overpressure protection for this class of faults.

56 In performing the transient analysis, EDF and AREVA have 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. They also claim to have modelled sensitivity studies to the worst single failure in the reactor engineered safety features, which for the feed line break fault is either that one of the EFWS pumps fails to operate or one of the valves on the MSRT system fails to open. On the basis of the analysis presented, EDF and AREVA have concluded that the EFWS and the MSRT systems provide 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

57 EDF and AREVA have considered the following faults within this category that they consider to be limiting and which are presented within the PCSR:

- turbine trip;
- loss of condenser vacuum and other events resulting in turbine trip;
- loss of external electrical load;
- loss of normal feedwater flow;
- inadvertent closure of main steam isolation valves;
- feedwater system pipe break.

58 All the above events are considered to be PCC-2 events, with the exception of the inadvertent closure of the main steam isolation valves which is considered a PCC-3 event and a feedwater system pipe break, which is considered to be a PCC-4 event. I have chosen to sample the last three faults listed above on the grounds that feedwater system piping failure is the most limiting fault according to EDF and AREVA, and the loss of normal feedwater flow and the closure of the main steam isolation valves are judged to be the most bounding of the more frequent faults in terms of the reliability requirements for the MSRT, MSSV and the EFWS systems.

59 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 PSA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

60 The feedwater system piping failure assessment assumes the rupture of a main feed line. EDF and AREVA claim that the initiating frequency for this PCC-4 design basis event is less than 1×10^{-4} per year. Given that this is a passive failure, this frequency appears to be reasonable. 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.

61 EDF and AREVA have indeed treated the fault as within the design basis and have identified what they consider the most onerous single failures (failure of one of the EFWS pumps or failure of one of the MSRT relief valves). Clearly, the failure of either an EFWS pump or an MSRT valve to operate will reduce the rate at which decay heat can be removed from the primary circuit such that the claim that these are the bounding single failures appears plausible given that the protection signals that are claimed are all based upon 2-out-of-4 voting logic. However, the Pressuriser Safety Relief Valves (PSRVs) 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, EDF and AREVA regard this as being covered by the PCC-3 design basis event, 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 there is a need for this to be demonstrated by EDF and AREVA in Step 4.

62 The assumption about whether a consequential loss of grid occurs as a result of a reactor trip needs careful consideration for these transients. This is because loss of grid results in the RCPs coasting down. When operating, the RCPs contribute extra heating that is comparable to the level of decay heating. On the other hand, tripping the RCPs results in natural circulation cooling which reduces the amount of heat removed from the primary circuit and so increases the average core temperature. The PCSR argues that for the single failure case involving loss an EFWS pump it is conservative to assume the RCPs remain running since this increases heat removal requirements of the one remaining EFWS pump. For the single failure case involving the failure of an MSRT valve to open, it is conservative to assume the RCPs are tripped since this minimises the transfer of heat from the primary circuit and so maximises the thermal expansion of the primary coolant. I judge these arguments to be sensible.

63 In Fig. 8 of Section 14.5.3 of the PCSR, the pressuriser pressure transient as calculated by EDF and AREVA using the CATHARE computer code is presented for the feedline break fault. The calculations are for the 4250 MWth design for EPR. Similar analysis for the 4900 MWth design is provided in Appendix 14B of the PCSR although none is presented for the 4500 MWth case that is applicable for the UK EPR. The analysis assumes the loss of a single EFWS to account for the single failure criterion as required by SAP FA.6, EDR.2 and EDR.3. A second EFWS pump is also assumed to be unavailable due to preventative maintenance as required by SAP FA.6. The resultant pressuriser pressure transient shown in Fig. 8 is seen to be doubly peaked. The initial peak occurs early in the transient and is due to the loss of feed caused by the feedline break reducing the amount of heat taken out by the steam generators. This causes the primary circuit to heat-up until the reactor is tripped on low steam generator water level. The rise in peak pressure is sufficient to cause the PSRVs to open. Following reactor trip the primary circuit cools and the PSRVs close. The remaining intact steam generators also start to dry out. This causes the second peak in the primary pressure as the circuit heats up again. The PSRVs re-open and the pressuriser level will start to rise as the

water in the primary circuit expands as it heats up. Flow from the EFWS is initiated on low steam generator water level.

64 The pressuriser water volume transient for the feedline break fault is not presented within the PCSR although it is the key transient for determining the adequacy of the sizing of the EFWS pumps that are claimed for this fault. EDF and AREVA have identified that a single EFWS pump does not have sufficient heat removal capacity to prevent the pressuriser from becoming water solid. Instead, after one hour, operator action is required in order to reconfigure the EFWS to provide additional flow from an extra EFWS pump. In response to a TQ, EDF and AREVA have accepted that there is little margin on the water level after one hour such that the pressuriser level would become water solid after a further 15 minutes delay. It is noted that the design flow from the EFWS to a single steam generator is 25 kg/s (90 te/h) at these fault conditions. EDF and AREVA have confirmed that the need for operator action could just be avoided if the flow from the EFWS pumps was to be increased to 33 kg/s (120 te/h). If the design intent is such that the EFWS flow rate should provide sufficient heat removal capability to match the heat input into the primary circuit after thirty minutes, so as to avoid steam generator dryout, then the flow from the EFWS pumps would need to increase to 44 kg/s (158 te/h). The auxiliary feedwater flow from a single pump to a pair of steam generators on Sizewell B (Ref. 11) is 32 kg/s (114 te/h). Given that the thermal power of the UK EPR at 4500 MWth is 30% greater than that of Sizewell B at 3411 MWth and scaling the auxiliary feedwater flow rate in proportion gives a required flow rate of 41 kg/s (148 te/h) which compares reasonably well with the EDF and AREVA estimate.

65 Most safety systems on Sizewell B are provided with four-fold redundancy. The design basis assumption (Ref. 11) 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. However, there are exceptions to this principle for the auxiliary feedwater system on Sizewell B. The four auxiliary feedwater lines to the steam generators are paired together into two common headers. Sizewell B therefore requires feed from 2-out-of-4 auxiliary feedwater pumps (Ref. 11) to ensure adequate post-trip heat removal following a feedline break fault. There is another exception; the minimum heat removal requirements following an ATWT event are that 3-out-of-4 trains of the auxiliary feedwater system should be available. For all other faults, the Sizewell B auxiliary feedwater system is able to meet the minimum cooling requirements with only 1-out-of-4 trains available. In the case of the UK EPR, none of the EFWS trains share a common header but the capacity of the pumps means that 2-out-of-4 feed pumps are required following a feedline break fault unless operator action is to be claimed after one hour to realign the system. In effect, both reactor designs are making a time at risk argument to exclude the need to consider an additional preventative maintenance given the initiating frequency for the feedline break fault. Given the ALARP precedent set by Sizewell B, it would be difficult to justify making EDF and AREVA increase the flow capacity of the EFWS pumps unless the EFWS system fails to meet the 1-out-of-4 requirements implied by SAPs FA.6, EDR.2 and EDR.4 for the more frequent loss of feed fault discussed below.

66 The inadvertent closure of all of the MSIVs fault places the greatest demands on the reliability of the primary and secondary overpressure protection. EDF and AREVA have classified this as a PCC-3 event which means it could be as frequent as 1×10^{-2} per year for which the expectation would be that a diverse means of protection would be provided. For protection against such faults the UK EPR is provided with three pilot operated Pressuriser Safety Valves (PSVs). This contrasts markedly with the situation at Sizewell B which is provided with three Pilot Operated Safety Relief Valves (POSRVs) and a diverse set of two 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. It also recognises the higher consequential failure probability of the POSRVs failing to open as compared with the simpler spring loaded valve design. In providing a diverse set of safety valves on the primary side, Sizewell B is protected against a potential common failure of one set of pressuriser relief valves for frequent faults.

67 The analysis for these faults is presented within Section 14.4 of the PCSR which considers PCC-3 events. However, the Chapter 14 analysis focuses on the issue of DNB during the pre-trip phase of the transient, referring to work reported in Appendix 14B for the 4900 MWth EPR design. The overpressure protection aspects of the fault are presented separately in Chapter 3.4 of the PCSR. Cases are presented for both the primary side and the secondary side overpressure transients using the MANTA computer code. The results include sensitivity studies for the single failure of a single PSV on the primary side and the single failure of one of the two MSSVs on the secondary side. The MSRT system is assumed to fail. The key feature is that the reactor protection system is being claimed to trip the reactor to mitigate the effects of the transient rather than relying solely upon the capacity of the relief valves to provide for 100% flow conditions. On the secondary side the MSRT system together with the MSSV system is sized to provide 100% flow so the situation is probably acceptable. The UK EPR design also provides for the isolation of these valves which is probably an advantage for cooldown faults discussed earlier and the steam generator tube rupture faults discussed below. However, on the primary side there appears to be no diverse safety system to protect against the common mode failure of the PSVs. This issue will need to be discussed with EDF and AREVA in Step 4.

68 EDF and AREVA have identified that the loss of normal feedwater fault is a PCC-2 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 EDF and AREVA 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;
- reactor trip;
- opening of the safety relief valves on the primary and secondary circuits;
- initiation of the EFWS;
- isolation of steam systems;
- closing of the safety relief valves on the primary and secondary circuits.

69 As an example, EDF and AREVA need to consider performing sensitivity studies in which 1) common mode failure of the EFWS is assumed and 2) common mode failure of the MSRT system is assumed. 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. Note that the common mode failure of the EFWS is discussed further below.

70 Although EDF and AREVA have identified that the loss of normal feedwater fault is a PCC-2 event, no design basis analysis is presented for the fault within the PCSR even though this is a much higher frequency event than the feedline break discussed previously. The only significant difference is that all four steam generators are intact and so they all contain water during the early stages of the transient. However, unless EDF

and AREVA are arguing that two EFWS pumps are available for cooling after assuming one pump is unavailable due to preventative maintenance and another fails due to a single failure, it is not clear that adequate cooling is available. In my judgement, the extra water in the steam generators is only likely to delay the transient compared with the feedline break case. It will not eliminate the possibility of steam generator dryout or significantly alter the margin to fill on the pressuriser water level if only one EFWS pump is available. In order to have two EFWS pumps available, EDF and AREVA will need to argue that the loss of feed fault initiating event is not capable of also failing one of the four EFWS trains. It must also be recognised that a 2-out-of-4 system will have a lower reliability than a 1-out-of-4 system. These issues will need to be raised with EDF and AREVA in Step 4.

71 From a systems perspective, the UK EPR has the potential to claim two diverse feed systems; the EFWS which provides feed to the steam generators, and bleed and feed using the safety injection system that requires manual operation to depressurise the reactor. The motive power for the EFWS pumps is taken from the AC essential electrical system which is backed up by four diesel generators should there be a loss of off-site power in coincidence with the reactor trip. Two manually operated station blackout diesels are provided for two of the EFWS pumps should the diesel generators undergo a common mode failure. These need to be started within 1.5 hours of the start of the fault. In contrast, Sizewell B has three diverse feed systems, feed to the steam generators from the motor driven auxiliary feedwater system, feed to the steam generators from the steam-turbine driven auxiliary feedwater system, and bleed and feed using the safety injection system which requires manual operation like on the UK EPR. While the station blackout diesels provide some diversity to the failure of the four main diesel generators, they are clearly not as functionally diverse as the steam driven auxiliary feedwater system which is driven by steam stored in the steam generators. This issue will need to be explored further with EDF and AREVA in Step 4. At a minimum, an ALARP justification will be required for not providing a diverse set of steam turbines.

72 Given that the loss of feedwater fault is a frequent PCC-2 event, there is also a need to consider the common mode failure of the EFWS for reasons other than the total loss of all electrical supplies. EDF and AREVA claim that bleed and feed provides this diverse protection. The expectation in the UK is that such analysis would be performed within the design basis analysis using conservative assumptions to allow for uncertainties. However, the total loss of feedwater case including the total loss of the EFWS is presented as a risk reduction sequence in the RRC-A analysis in Chapter 16.1 of the PCSR. In principal, EDF and AREVA procedures permit this analysis to be performed on a best estimate basis including the choice of initial conditions and the allowance on claims on the CVCS letdown and charging systems. However, in practice, EDF and AREVA have chosen to consider single failures for one of the PSVs failing to open and for one of the MHSI trains failing to operate. They have also not claimed operator action for the first 30 minutes. Since the construction of Sizewell B, the single failure criterion in SAP EDR.4 has been changed in that the single failure applies to the safety function and not to a safety system. Given that the EFWS provides a diverse means of achieving the safety function to that of bleed and feed it is probably not necessary to consider these additional single failures to be within the design basis. I would be interested in further sensitivities being performed on the effects of the best estimate assumptions for the initial conditions and the effects of not claiming the CVCS. These issues will need to be discussed further with EDF and AREVA in Step 4.

73 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 the requirements of the French Safety Authority. As noted above, an assessment needs to be made against the UK requirements given in SAPs FA.3, FA.7 and Target 4 during Step 4. However, I judge that any differences are

likely to be minor due to methodological assumptions and it is unlikely to require additional protection measures for these faults.

74 The EDF and AREVA analysis uses the CATHARE computer code to model the feed line break fault and the THEMIS and FLICA codes to model the MSIV closure transients while the overpressure analysis reported in Chapter 3.4 of the PCSR uses the MANTA code. The validation evidence for these codes against SAPs FA.17 to FA.22 has not been assessed in detail in Step 3 although the CATHARE code is discussed further in Section 2.2.2.6.5. For the Step 4 assessment, I will review the validation evidence supporting the calculational route.

75 No discussion is presented within the analyses about the possibility of consequential failures such as a stuck open pressuriser safety relief valve failing to close 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 requirements for the EFWS and MSRT systems are adequate. Nevertheless, from a response to a TQ, it is understood that the conditional failure probability for a primary safety relief valve failing to close having opened is assumed in the PSA to be 2.5×10^{-2} per demand, and so 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. EDF and AREVA appear to be in the process of reviewing this reliability data and so this issue will need to be explored further with EDF and AREVA during Step 4.

2.3.2.3 Decrease in Reactor Coolant System Flow Rate Faults

2.3.2.3.1 Summary of Requesting Party's Safety Case

76 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.

77 The basis of the EDF and AREVA safety case is that they have reviewed a number of postulated events that they consider to be within the design basis of the plant and that could result in a decrease in the reactor coolant system flow rate. For those cases which they consider to be limiting they have performed detailed analyses and claim 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.

2.3.2.3.2 ND Assessment

78 EDF and AREVA have considered the following faults within this category that they consider to be limiting and which are presented within the PSCR:

- 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.

79 The first event is a PCC-2 event, the second a PCC-3 event, and the last two events are PCC-4 events according to the classification scheme of EDF and AREVA. I have chosen to sample the second fault listed above because it is one of the most limiting faults to protect against in terms of the DNB criteria. In addition, although it is a PCC-3 event, loss of electrical supplies to the pumps is a possible cause of the fault and I judge that the initiating frequency could be close to that of a PCC-2 event and yet the design rules of EDF and AREVA would allow DNB and limited fuel rod damage to be conceded for the fault.

80 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 PSA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

81 The fault that is being sampled is the loss of reactor coolant flow as a result of the simultaneous coasting down of all four RCPs. The fault is treated as a design basis transient and so meets the requirement of SAP FA.5. There 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 whereas it is only discussed within the RRC-A analysis. This is a generic issue and is discussed in the section on ATWT faults presented below. The present analysis is therefore judged to only partially meet the requirements of SAPs FA.6, EDR.2 and EDR.3 on the need for diversity and so this issue will need to be discussed with EDF and AREVA in Step 4.

82 The analysis results for DNB are summarised in Fig. 4 of Section 14.2.6 of the PCSR's Appendix 14B which illustrates the DNBR 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 EDF and AREVA have applied to its DNB correlations against the validity of assurance SAPs FA.17 to FA.22. A TQ has already been raised with regard to the treatment of uncertainties within the DNB methodology and this will need to be explored further. 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 and 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.

83 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 the French Safety Authority requirements. An assessment needs to be made against the UK requirements given in SAPs FA.3, FA.7 and Target 4 during Step 4 although I judge that any differences are likely to be minor due to methodological assumptions and it is unlikely to require additional protection measures for these faults.

84 The EDF and AREVA analysis uses the PANBOX and COBRA-3 computer codes to model these decreases 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

85 Faults in this category cause the fuel to generate power in excess of the cooling provisions. Such faults can be bought 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.

86 The basis of EDF and AREVA safety case is that they have reviewed a number of postulated events that they consider to be within the design basis of the plant and that could result in reactivity and power distribution anomalies. For those cases which they consider to be limiting they have 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.

87 In performing the transient analysis, EDF and AREVA have, 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, EDF and AREVA have concluded that adequate protection is provided for all the range of faults considered.

2.3.2.4.2 ND Assessment

88 EDF and AREVA have considered the following faults within this category that it considers to be limiting and which are presented within the PCSR:

- uncontrolled RCCA bank withdrawal at power;
- uncontrolled RCCA bank withdrawal from hot zero power;
- RCCA misalignment up to rod drop, without limitation;
- start-up of an inactive reactor coolant pump at an incorrect temperature;
- chemical and volume control system malfunction that results in a decrease in boron concentration in the reactor coolant;
- uncontrolled single control rod withdrawal;
- inadvertent loading and operation of a fuel assembly in an improper position;
- spectrum of RCCA ejection faults.

89 Most of the faults listed above are PCC-2 events. Inadvertent loading is a PCC-3 event while RCCA ejection faults are a PCC-4 event. RCCA misalignment includes both PCC-2 and PCC-3 events. I have chosen to sample three of the above fault types. The first fault type 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 type is RCCA misalignment faults on the grounds that a diverse means of protection is required should the in-core protection system suffer a common mode failure recognising that it is difficult to detect and provide automatic protection for these faults. The third fault type is the rod ejection fault which EDF and AREVA judge 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 fuel misloading of a large number of fuel assemblies will need to be explored following the operational incident at Dampierre-4 (Ref. 32) in France.

90 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 PSA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

91 The uncontrolled withdrawal of an RCCA bank at power fault is a PCC-2 event and is treated as a design basis transient so meeting the requirement of SAP FA.5. EDF and AREVA claim 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 whereas it is only discussed within the RRC-A analysis. This is a generic issue and is discussed in the section on ATWT faults presented below. The present analysis is therefore judged to only partially meet the requirements of SAPs FA.6 and EDR.2 and EDR.3 on the need for diversity and so this issue will need to be discussed further with EDF and AREVA in Step 4.

92 To aid my judgement of the uncontrolled RCCA bank withdrawal fault, I have benchmarked the analysis approach adopted by EDF and AREVA against the safety case analysis for Sizewell B (Ref. 13) 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.

93 EDF and AREVA claim that the following protection systems are available to protect against this fault:

- reactor trip on low DNBR protection (in-core detectors);
- reactor trip on high neutron flux rate of change (ex-core detectors);
- reactor trip on linear power density protection (in-core detectors);
- reactor trip on high core power;
- reactor trip on high pressuriser pressure;
- reactor trip on high pressuriser level.

94 The low DNBR trip parameter is derived from measurements of the pressuriser pressure, the coolant cold leg temperature, RCP speed, and information from the in-core neutron detectors. The linear power density signal is based on the in-core neutron detectors. The high core power level trip parameter is based upon measurements of the pressuriser pressure and the coolant hot and cold leg temperatures. Interestingly, in contrast with the position at Sizewell B, no reactor trip signal is provided on high neutron flux level using the power range ex-core detectors although in principle these would be able to provide protection against these faults for at least some of the reactivity insertion speeds.

95 The analysis results are summarised in Fig. 14 of Section 2.10 of the PCSR's Appendix 14B of the PCSR which presents the minimum DNBR as a function of reactivity insertion rate for the minimum reactivity feedback coefficient at 100% power. 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.

96 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 roughly equivalent the low DNBR trip on the UK EPR although it is based upon the N-16 detectors rather than the in-core detectors, is not claimed. The N-16 system is provided for over power trip protection against cooldown 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 UK EPR does not possess such a system but it does possess in-core detectors which are connected to the protection system and so can trip the reactor automatically. Hence, in principle, there appears to be diversity to the high flux rate of change reactor trip protection on the UK EPR, meeting the requirements of SAP ESS.7 although both systems are currently connected to same digital Reactor Protection System (RPS). The reason why no high flux power range trip signal is provided will need to be explored with EDF and AREVA.

97 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 (Ref. 13). The only reactor trip parameters plotted by EDF and AREVA on Fig. 14 are the high flux rate of change and low DNBR 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 low DNBR is seen to be in-effective 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.

98 There is no discussion of PCI failures as a result of the reactivity insertion faults within the EDF and AREVA analysis although as noted in the ND fuel assessment report (Ref. 7), this is an area where it is understood that EDF and AREVA are performing further work. On Sizewell B (Ref. 13) the need for protection against PCI for frequent faults with an initiating frequency greater 1×10^{-3} per year is an accepted design criteria for the fuel. In my judgement, it is reasonable to expect the UK EPR to also meet this requirement particularly since it is proposed that the fuel will operate to a lower linear rating than that for Sizewell B. Furthermore, the UK EPR is also provided with in-core detectors that are connected to the protection system to provide an automatic trip signal. 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 using the ex-core detectors (Refs 14 and 15) but the system was never implemented because Sizewell B was able to demonstrate sufficient margin with its current protection system. In my judgement, the provision of in-core detectors on the UK EPR that are connected directly to the reactor protection system potentially represents a significant safety improvement over the ex-core detectors that were provided on earlier PWR designs such as Sizewell B.

99 In summary, EDF and AREVA, 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. This issue will be raised as an RO.

100 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.

101 I have chosen to sample the withdrawal of a single RCCA fault as this is a PCC-3 event for which the EDF and AREVA design criteria would allow a limited amount of fuel rods to

undergo DNB. However, EDF and AREVA claim that the low DNBR trip is very effective for this fault such that in practice DNB is avoided. Nevertheless, as this is potentially a frequent fault with an initiating frequency that could be as high as 1 x 10^{-2} per year, there is a need to demonstrate a diverse means of detecting the fault should the low DNBR trip system be subject to a common mode failure. It is noted that the primary protection system for Sizewell B is fitted with specific 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. This issue will need to be further explored with EDF and AREVA during Step 4 including the issue of ramp and hold faults.

102 RCCA ejection accidents are defined as the mechanical failure of the pressure housing of an 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.

103 EDF and AREVA have treated the fault as an infrequent PCC-4 event with an initiating frequency that can range as high as 1 x 10^{-4} per year. As this is a passive failure this seems reasonable and meets the requirements of SAP FA.5. EDF and AREVA claim 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.

104 To aid my judgement of these faults, I have benchmarked the analysis approach adopted by EDF and AREVA against the original safety case analysis provided in support of the Sizewell B PCSR (Ref. 16) 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.

105 The analysis results are summarised in Table 2 of Section 14.5.5 of the PCSR which presents a summary of the key physics parameters for a range of initial reactor powers including hot full power and hot zero power cases for end of cycle conditions. The parameters include the predicted maximum rod worth insertion, the maximum fuel enthalpy and the maximum temperatures of the fuel and cladding. The calculations were performed using the 3-D SMART neutronics computer code and the FLICA thermal hydraulics computer code. For hot full power conditions the reactivity worth of the ejected rod is 0.135 Niles, the peak centre fuel temperature is predicted to be 1972ºC and the maximum fuel enthalpy rise is predicted to be 93.1 Cal/g. The peak fuel enthalpy occurs at 42% power and is 116 Cal/g.

106 It is interesting to compare the results of the EDF and AREVA analysis with the Sizewell B analysis (Ref. 16) for the hot full power condition for which results are available. The Sizewell B analysis also performs an explicit 3-D calculation using TWINKLE. The reactivity worth of the ejected rod is predicted to be 0.120 Niles, the peak centre fuel temperature is predicted to be 1799ºC and the fuel enthalpy is predicted to be significantly less than 140 Cal/g. These results give reasonable confidence in the UK EPR analysis which suggests that the rod bank insertion limits for UK EPR 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. 7) that the Radial Averaged Peak Fuel Enthalpy (RAPFE) safety limit against which the peak fuel enthalpy is assessed needs to be revised by EDF and AREVA. 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 the requirements of the French safety authorities. During Step 4 it will be necessary for such an assessment to be made against the UK requirements given in SAPs FA.3, FA.7 and Target 4 although I judge that any differences are likely to be minor due to methodological assumptions and it is unlikely to require additional protection measures for these faults.

108 The EDF and AREVA analyses use the SMART, THEMIS, FLICA and COMBAT 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. 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 EDF and AREVA safety case is that they have reviewed a number of postulated events that they consider to be within the design basis of the plant and that could result in an increase in the reactor coolant inventory. A single case is identified which is considered to be limiting and for which it is argued that the reactor protection system is able to isolate the fault without the need for a reactor trip.

2.3.2.5.2 ND Assessment

111 EDF and AREVA have considered the following fault within this category that they consider to be limiting and which is presented within the PCSR:

- CVCS malfunction that increases reactor coolant inventory.

112 This is a PCC-2 event according to the classification scheme of EDF and AREVA.

113 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 PSA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed.

114 EDF and AREVA have identified that a CVCS fault causing an increase in reactor coolant inventory is a PCC-2 event and so it needs to be treated as a design basis event to meet the requirements of SAP FA.5. Isolation of the CVCS charging line and opening of the CVCS letdown lines are claimed to protect against this fault although it is understood that only the former are to be qualified to F1 standard. EDF and AREVA assessment procedures for the analysis of PCC-2 faults only allow F1 systems to be claimed for such faults, which is consistent with UK requirements as explained in SAP FA.6. As a frequent event it needs to be treated within the traditional UK approach to design basis analysis which requires two diverse safety systems, qualified to an appropriate standard, to be provided for each safety function as required by SAPs FA.6, EDR.2 and EDR.4.

115 No discussion is presented within the analyses about the possibility of consequential failures such as a stuck open PSRV resulting in a consequential LOCA should the pressuriser become water solid. This is perhaps appropriate given this design basis

section is attempting to demonstrate that the adequacy of the protection system to prevent the pressuriser becoming water solid. Nevertheless, given that the conditional failure probability for a safety relief valve to close could be as high as 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 and the common mode failure probability of the protection system. This issue will need to be explored further with EDF and AREVA during Step 4 of the GDA.

2.3.2.6 Decrease in Reactor Coolant Inventory Faults

116 The assessment of EDF and AREVA's safety case for decrease in reactor coolant inventory faults has been split into four areas:

- SGTR;
- SBLOCA;
- IB and LBLOCA (within the design basis);
- 2A-LBLOCA.

2.3.2.6.1 Summary of Requesting Party's Safety Case for SGTR

117 Two design basis SGTR faults are considered in the PCSR. The double-ended rupture of a single SG tube is identified as a PCC-3 design basis incident (i.e. an initiating frequency between 1 x 10^{-4} per year and 1 x 10^{-2} per year). The double-ended rupture of two SG tubes is identified as a PCC-4 design basis accident (i.e. an initiating frequency between 1 x 10^{-6} per year and 1 x 10^{-4} per year).

118 The PCSR describes a number of SG design features that have been included to reduce the probability of a SGTR event, including the choice of a ductile SG tube material, the location of the blowdown system at the bottom of the SG tube bundle, chemistry control of the secondary water, and activity control of the water on the secondary side within defined limits.

119 The EDF and AREVA approach is to subdivide the transient into short term and long term to separate the phases of reactivity release to the atmosphere. The short term phase is defined as up to the point of leak termination. This includes the controlled state in which the leak is compensated for by the Reactor Coolant System (RCS) injection. In the long term phase, the plant is transferred to the safe shutdown conditions with a possible activity release if depressurisation of the affected SG by the MSRT is required.

120 The loss of primary coolant causes a decrease in the primary pressure and contamination of the secondary side. A reactor trip is assumed to occur on "PZR pressure < MIN2" or a "SG level > MAX1" signal generated of the affected SG. The reactor trip automatically trips the turbine and the SG pressure rapidly increases. The Main Steam Bypass (MSB) to the condenser is assumed to be unavailable as it is not F1-classified. It would also not be available following a Loss Of Offsite Power (LOOP) occurring at the time of turbine trip. Therefore, contaminated steam is assumed to be discharged to the atmosphere when the MSRTs pressure setpoints are reached.

121 The continuous loss of RCS coolant inventory causes the pressuriser to empty. For the design basis faults, this results in a depressurisation of the primary side because the CVCS is not able to match the break flow.

122 Upon the receipt of a Safety Injection (SI) signal on either "PZR pressure < MIN3" or "SG level > MAX2" from the affected SG, the EPR design causes a deliberate partial cooldown of the RCS to lower the pressure sufficiently to allow injection from the MHSI

pumps. This cooldown is performed using the secondary side and consists of the C&I system decreasing the MSRT setpoint of the four SGs from 95.5 bar to 60 bar, at a rate giving a cooldown of 250°C/h (at the same time, the MSB setpoint is decreased from 90 bar to 55 bar at the same rate although this is not claimed in the analysis).

123 The MHSI pumps are actuated following the SI signal but they do not inject until the primary pressure has dropped to the range ~85 to 97 bar.

124 The controlled state is reached when the MHSI injection and CVCS (if available) are able to match the SGTR flow rate. However, at this point the affected SG continues to fill with contaminated water and activity release to the atmosphere continues.

125 From the controlled state, the affected SG is identified and isolated automatically (or manually if the operator can respond before the high SG level setpoint is reached). The isolation involves raising the MSRT setpoint above the MHSI shutoff head (but below the MSSV pressure setpoint) and closing the MSIV. The isolation of the affected SG causes the flow via the break to increase the pressure in the affected SG. Once the primary and secondary side of the affected SG pressures equalise, the flow via the break is terminated.

126 This is defined in the PCSR as the end of the short term phase, a state which can be achieved using only automatic F1 signals and systems.

127 The safe shutdown state is defined as a state where the affected SG is isolated and one Safety Injection System / Reactor Residual Heat Removal System (SIS / RHRS) train connected to the RCS. The transition from leak termination to the safe shutdown state is defined in the PCSR as the long term phase. To achieve the safe shutdown, the operator is required to initiate boration via the EBS and cooldown the RCS using the unaffected SGs.

128 At the end of the RCS cooldown, the RCS pressure (with the MHSI still on) is higher than the Low Head Safety Injection (LHSI) maximum connecting pressure. To lower the pressure, the MSRT on the affected SG is opened. However, if the affected level is too high, the operator first opens the transfer line (a safety grade component of the SG blowdown route) between the affected SG and its partner SG to lower the level. This prevents overfilling the affected SG and the risk of a large activity release to atmosphere.

129 The claimed systems and operator actions required to transfer to the safe shutdown state are all at least F1B. No operator action is claimed before 30 minutes after the reactor trip. This is extended to 1 hour if local operator action is needed.

130 Transient analysis is presented (separately) in the PCSR for the short term and long term phases. Cases without LOOP from a pre-trip power of 102% have been undertaken to evaluate the maximum amount of activity released to the environment, and with LOOP from a pre-trip power of 2% to demonstrate that no SG overfilling (and therefore no liquid is released to the environment prior to leak termination).

131 The PCSR states that the cases without LOOP are new calculations performed within the framework of GDA. They have been done with the CATHARE code for a 4500 MWth EPR.

132 The cases with LOOP have been taken from pre-existing analysis undertaken for a 4900 MWth EPR design which has been presented in Appendix 14B of the PCSR. S-RELAP5 has been used for this analysis. The PCSR contains discussion on the applicability of 4900 MWth analysis to the UK EPR. The available analysis for the short term phase of the two tube rupture with LOOP case has been further supplemented by analysis presented in the Flammaville Preliminary Safety Analysis Report (PSAR) report for a 4250 MWth reactor (Ref. 17).

133 The design basis analysis has clearly identified the choice of limiting single failure and any systems assumed unavailable due preventative maintenance.

134 Using the presented transient analysis to support its claims, the PCSR concludes that for both design basis faults (one and two tube ruptures) the controlled state can be achieved using only F1A systems, and the safe shutdown states using only F1A and F1B systems. In addition, it claims that even with the worst single failures and preventative maintenance, no demand is placed on the MSSV and the affected SG will not overfill. The affected SG pressure is kept below or equal to the RCS pressure and therefore any SGTR reverse flow is negligible (i.e. no criticality risk). The core always remains covered.

135 For PCC-3 and PCC-4 faults, the PCSR sets the numerical dose targets of 10 mSv for effective dose and 100 mSv for equivalent thyroid dose. Using the short and long term phases combined steam release masses from calculated from 102% power no LOOP analysis, the PCSR presents effective dose values, for the notional limiting individual, not exceeding 170 μSv.

2.3.2.6.2 ND Assessment of SGTR Safety Case

136 The design basis analysis presented in the PCSR for the both the single tube and two tube rupture faults appears systematic and thorough, in accordance with SAP FA.4. In Step 4, the detailed calculations and the PCSR's supporting references will be assessed.

137 The transient analysis that is presented supports the claims that EPR's automatic F1A systems can achieve the identified controlled state and leak termination point, and that F1A and F1B systems and operator actions can achieve the cold shutdown state following the fault.

138 I judge the identification of a single tube rupture as a PCC-3 design basis incident and a double tube rupture PCC-4 design basis accident, with the associated initiating frequencies to be sensible. There is no discussion as to why more severe faults need not be considered within the design basis (i.e. 3+ tube ruptures). I intend to ask EDF and AREVA in Step 4 to produce evidence showing that more severe faults need not be considered but this is unlikely to require additional faults being added to the fault schedule or for further transient analysis.

139 The fault sequences for the two design basis faults are clearly presented and discussed in the PCSR. The assumptions made in the analysis with respect to plant state, system availability, single failures, preventative maintenance etc. are unambiguously set out.

140 The ability to automatically depressurise the reactor, detect the affected SG and terminate the leak with margin to overfill is a notable feature of the UK EPR design and an improvement on many operating PWR designs. This ability is enabled by design choice of MHSI pumps (as opposed to high head pumps) and the deliberate depressurisation of the RCS to a pressure below the operating head of the MHSI. While the benefit to SGTR faults is welcomed, it is recognised that the design choice of MHSI has potential adverse implications for the management of IBLOCA faults.

141 The depressurisation of the RCS is achieved by the release of steam to the atmosphere from the SGs via the MSRTs (assuming the steam cannot be dumped to the non-F1 condenser). This includes the deliberate release of contaminated steam from the affected SG. It is known that an earlier design of the Finnish EPR adopted a different management strategy for tube rupture faults which minimised the release to atmosphere from the affected SG. However this approach increased the risk of a heterogeneous dilution of the RCS from the secondary side. As a result, the latest Finnish approach includes a partial cooldown similar to that proposed in the UK. I recognise that accepting some atmospheric release to reduce the risk of a reactivity insertion is a necessary trade off. Having pursued this matter via a TQ, I understand the design choices that have been made. However, I still wish to explore further with EDF and AREVA whether there are other options that could be considered to reduce the risk to ALARP. I also wish to pursue

further the design choices made to reach the safe shutdown state, exploring whether activity introduced to parts of the secondary side and released to atmosphere is ALARP.

142 The cooldown rate of the partial cooldown is assumed in the design basis transient analysis to be 100°C/h but EDF and AREVA have confirmed via a TQ (Ref. 18) that at the end of the 2008 design freeze, the RCS partial cooldown rate for UK EPR is 250°C/h. The maximum blowdown rate of the MSRT is believed to be approximately 450°C/h. A faster blowdown rate increases the margins for LOCA events but also increases the mechanical stress on the structures of the primary circuit. The PCSR explicitly discusses the impact of a 250°C/h rate compared to the assumed 100°C/h, stating that the impact on SGTR studies is small. With respect to Step 3 and SGTR faults, I am happy with the appropriateness with intended partial cooldown rate and the assumed rate in the design basis analysis. In Step 4, EDF and AREVA will be asked to provide further evidence of this lack of sensitivity of transient analysis to the assumed cooldown rate.

143 The PCSR makes claims on the F1A "PZR pressure < MIN2" or a "SG level > MAX1" signals (which one being depended on the power state) to detect an SGTR, trip the reactor and initiate the sequence of events which results in the fault being adequately dealt with. However it is know that the Finnish EPR also makes claims on a F1A activity signal in a main steam line to automatically trip the reactor following a SGTR (Ref.19). No automatic trip on activity is credited for the UK EPR although a manual F1B trip is claimed. Given that the Finnish EPR is potentially setting good practice and appears to be showing that an automatic activity trip is a practicable measure to implement, EDF and AREVA have not currently demonstrated why the UK EPR approach is ALARP. In Step 4, I will raise a TQ asking EDF and AREVA to clearly state why the proposed approach for the UK EPR is ALARP.

144 The thermal hydraulic analysis of SGTR faults has been undertaken with either S-RELAP5 or CATHARE. Both codes have been subject to extensive verification and validation, which has been summarised in the PCSR. Both, if used correctly, should be appropriate for modelling SGTR faults. The validation of the codes will be investigated further in Step 4 but at this stage I have no indications that their use is problematic. I have discussed CATHARE further in Section 2.2.2.6.5.

145 The assessments to demonstrate a margin to overfill assuming LOOP have not been undertaken specifically for the UK EPR. The PCSR explicitly discusses the differences and the appropriateness of the 4900 MWth EPR analysis with respect to the proposed UK EPR design. However further consideration will be given in Step 4 to the applicability of these calculations to satisfy myself that UK EPR specific assessments are not necessary.

146 The stated radiological consequences for the two design basis SGTR faults appear to compare favourably with the Target 4 dose limits in the SAPs. However, the details of the calculations and their contained assumptions have not been examined in Step 3. In Step 4, in co-operation with ND Inspectors of different disciplines, the adequacy and appropriateness of the radiological consequences calculations will be assessed.

2.3.2.6.3 Summary of Requesting Party's Safety Case for SBLOCA

147 A SBLOCA with an equivalent diameter of 20 cm^2 (or smaller) in reactor States A & B is defined in the PCSR as a PCC-3 design basis incident (i.e. an initiating frequency between 1 x 10^{-4} per year and 1 x 10^{-2} per year). The break results in a loss of reactor coolant inventory beyond the capability of the CVCS and results in a decrease in primary system pressure and the pressuriser level.

148 The protection against the unmitigated consequences of the fault is similar to that described above for a SGTR fault. For the State A fault, a reactor trip is assumed to

occur of “low pressuriser pressure < MIN2”. The reactor trip signal automatically trips the turbine and closes the main feedwater system lines. In the design basis analysis, a loss of offsite power is assumed to coincide with the turbine trip. As the secondary side pressure increases, the MSRT valves open, allowing steam to be dumped to atmosphere (assuming the non-safety main steam bypass to the condensers is unavailable).

149 An SI signal is generated on “PZR pressure < MIN3”, automatically starting the MHSI and LHSI pumps. A deliberate partial cooldown of the RCS is also initiated to sufficiently lower the pressure to allow injection from MHSI pumps. This cooldown is performed using the secondary side and requires the C&I system to decrease the MSRT setpoint of the four SGs from 95.5 bar to 60 bar, at a rate giving a cooldown of 250°C/h.

150 For breaks of this size, at the end of partial cooldown the volume of water lost through the break is less than the volume of water being added by the MHSI and the steam production in the core due to decay heat. Depressurisation of the RCS therefore stops at the end of partial cooldown. The mass of the water lost through the break continues to exceed the mass added through the MHSI until the break flow eventually changes to single phase steam. The PCSR claims that this controlled state can be reached without unacceptable consequences claiming just F1A systems.

151 The safe shutdown state is reached from the controlled state using F1A and F1B actions. The F1B actions include manual operations but no claims are placed on them until 30 minutes after the reactor trip. A further RCS cooldown is manually initiated via the secondary side, either by decreasing the MSB or MSRT setpoints. The RCS is depressurised by switching off the MHSI injection when the conditions are sufficient for the LHSI to provide the required injection. Safe shutdown in maintained by controlling the RCS water inventory with one LHSI in SI mode, and by controlling the RCS temperature with one LHSI operating in RHR mode.

152 The RCS must be borated to keep the core subcritical throughout the transient during the transition to safe shutdown. For smaller breaks (<1 cm^2) the MHSI boration is not sufficient due to the low injection flow rate. The CVCS can provide boration if it is available. The CVCS on the UK EPR is to be qualified to F2 standard while the CVCS on Sizewell B is qualified to the equivalent of F1A standard. The injection of boron can compensate for the reactivity insertion resulting from the RCS cooldown. If the CVCS is not available, the F1A EBS needs to be manually actuated to inject enriched boric acid. The RCS cooldown rate is either 25°C/h or 50°C/h, depending on whether one or two EBS pumps are in operation.

153 The ability of the safety systems to meet the PCSR safety criteria for a PCC-3 event has been demonstrated with transient analysis undertaken with the CATHARE thermal hydraulic code. However, the transient analysis that is presented was not specifically performed for the 4500 MWth UK EPR.

154 The PCSR argues that analysis undertaken for a 4250 MWth EPR (Ref. 17) adequately demonstrates the capability to reach the controlled state. A 20 cm^2 break occurring at the cold leg pump discharge pipe at 102% power is considered, taking into account a coincident loss of power, the limiting single failure (loss of one Emergency Diesel Generator (EDG)) and the most onerous preventative maintenance activity (another EDG). A partial cooldown rate of 100°C/h is assumed in the transient analysis compared to the 250°C/h rate proposed for the UK. Significantly, no core uncovery is predicted and therefore no core heat-up occurs.

155 The capability to reach a safe shutdown state is demonstrated using analysis for a 4900 MWth EPR design (Appendix 14B of Ref.1) with similar assumptions to those made for the controlled state analysis. The core remains covered throughout the transient with the RPV level above the bottom of the cold / hot legs. Core subcriticality is maintained throughout the transient for a 20 cm^2 break by the MHSI pump and after the LHSI / RHR

connection by the LHSI pump operating in SI mode. An additional evaluation is presented in the PCSR showing that the EBS with the MHSI can provide sufficient boration for any break size and for any anticipated fuel cycle (including MOX fuel).

156 The design basis assessments of SBLOCA have been extended by considering individually the common cause failure of three safety systems through RRC-A best estimate accident analysis.

157 A SBLOCA with a failure of the partial cooldown signal has been considered. In this scenario the operator is required to perform a manual cooldown by decreasing the setpoint of the four MSRTs to 60 bar in one step. The operator is prompted to do this step on information of "core outlet temperature above 350°C" with "no implementation of partial cooldown". The RCS pressure drops rapidly (~100 seconds) from well above the secondary pressure of 90 bar to below 60 bar, with MHSI injection starting almost immediately. Non-bounding CATHARE analysis for a 4250 MWth reactor is summarised in the PCSR showing that the operator action can be delayed until approximately an hour after the initial break and the final state can still be reached with the identified LOCA acceptance criteria being met.

158 A SBLOCA without MHSI has been considered. The first part of this sequence is identical to that for a typical SBLOCA. However at the end of the partial cooldown, with the RCS at pressure approximately equal to the secondary side (i.e. 60 bar), the operator is required to initiate a further fast cooldown by decreasing the secondary side pressure. This is required to allow accumulator and LHSI injection. The operator is prompted to do this step on information of "core outlet temperature above 350°C" with "no MHSI". Non-bounding CATHARE analysis for a 4250 MWth reactor is summarised in the PCSR showing that the operator action can be delayed until approximately 1.4 hours after the initial break (approximately 1 hour after the completion of partial cooldown) and the final state can still be reached with the identified LOCA acceptance criteria being met.

159 SBLOCA without LHSI / RHR has been considered. With this system unavailable, the required final state can only be reached by manual initiation of the secondary side cooldown via the MSB at a rate of 50°C/h. Without this cooldown, the decay heat would largely be dissipated to the IRWST (via the break) and in the long term this could lead to loss of the MHSI. After cooldown, the heat removal of the RCS and the IRWST is ensured by the Containment Heat Removal System / Component Cooling Water System / Essential Service Water System (CHRS / CCWS / ESWS) cooling chain. The PCSR summarises non-bounding analysis undertaken with the coupled codes S-RELAP5 and COCO for a 4900 MWth reactor which shows that the final state can be reached with no core uncovery or clad rupture. The analysis assumes that a manual cooldown of the plant via the MSBs is performed 30 minutes after the initial SIS signal has been received. Four hours into the transient, manual actuation of the CHRS is assumed to remove the heat from the IRWST and limit the IRWST temperature.

2.3.2.6.4 ND Assessment of SBLOCA Safety Case

160 The design basis analysis for SBLOCA faults presented in the PCSR appears systematic and thorough in accordance with SAP FA.4.

161 The classification of SBLOCA as a PCC-3 event and IB/LBLOCAs as PCC-4 events on the basis of frequency of particular breach sizes has not been challenged in Step 3. The classification does seem to be, in part, driven by consequences; design basis analyses of breaks up to 20 cm^2 show no core uncovery but breaks over 20 cm^2 can result in core uncovery.

162 Other than the classification and the consequences of the faults, there does not appear to be any difference in methodology between the SBLOCA PCC-3 events and the design

basis IB/LBLOCA PCC-4. I have therefore deferred my assessment comments on SBLOCA to the assessment section below on IBLOCA and LBLOCA.

2.3.2.6.5 Summary of Requesting Party's safety case for IBLOCA and LBLOCA

163 Intermediate breaks (equivalent diameter greater than 20 cm^2) and large breaks (up to surge line breaks) in States A and B are considered together in the PCSR as PCC-4 design basis accidents (i.e. an initiating frequency between 1 x 10^{-6} per year and 1 x 10^{-4} per year). The 2A-break of hot or cold legs is not considered a design basis accident. The cases considered are:

- 45 cm^2 (∅ 75 mm) break in the RCP discharge pipe.
- 80 cm^2 (∅ 100 mm) break in the RCP discharge pipe.
- 125 cm^2 (∅ 125 mm) break in the RCP discharge pipe.
- 180 cm^2 (∅ 150 mm) break in the RCP discharge pipe.
- SIS line break (390 cm^2 - ∅ 225 mm) located in the cold leg.
- Surge line break (2 x 830 cm^2 - ∅ 2 x 325 mm) located in the hot leg.

164 The location of the breaks in the RCP discharge pipe is a pessimistic assumption to maximise the mass discharge rate.

165 The initial sequence of events, in terms of detection of a loss of inventory, reactor and turbine trip, partial cooldown and starting of the MHSI and LHSI pumps, is the same as that discussed above for a SBLOCA. For the smaller intermediate breaks, the RCS discharge via the break, still in the form of a liquid, does not remove sufficient volumetric flow to match the steam production in the core caused by the decay heat. Consequently, the RCS depressurisation stops at the end of the partial cooldown. While the MHSI flow is insufficient to compensate for the break flow, the RCS inventory continues to decrease. Subsequently, the break flow rate decreases as the void fraction in the cold legs increases.

166 Once the break flow changes to single-phase steam, the volumetric RCS balance between steam production due to core decay heat and break flow is completely changed and the break size is the dominant parameter in dictating the subsequent depressurisation.

167 For the smallest intermediate breaks, steam produced from the core is removed directly via the break and by condensation in the SG tubes. The RCS pressure (saturation pressure) remains slightly above the SG pressure. Larger breaks discharge sufficient steam to allow further RCS depressurisation without steam condensation in the SG tubes. In the longer term the heat transfer reverses between the primary and secondary sides. The RCS pressure continues to fall independently of the SG temperature, down to the accumulator actuation pressure and possibly the LHSI pressure setpoint.

168 The subsequent behaviour of the RCS water inventory depends on the balance between SI flow, MHSI, accumulators and LHSI, and the break flow rate.

169 The controlled state is reached when the RCS inventory is stable, the core power is removed via the break (and if necessary the SGs) and the core is sub-critical.

170 From the controlled state, transfer to RHRS conditions is generally not possible as there is not enough SIS injected flow to compensate for the break flow and hence flood the hot legs. In these circumstances, the PCSR defines the safe shutdown state as the core sub-critical (after xenon depletion), break flow matched by SIS flow, decay heat removed from the core, the break flow is at a temperature lower than the containment saturation

temperature limit and the heat is removed from the containment by the designated cooling chain.

171 To achieve safe shutdown following cold leg breaks, the operator is required to switchover from LHSI cold leg injection to LHSI hot leg injection. This limits the containment pressure increase in the long term, prevents boron precipitation inside the core and prevents boron dilution inside the IRWST.

172 The PCSR summarises the results of CATHARE calculations up to the controlled state undertaken for each of the identified LOCA cases for a 4250 MWth reactor. For each case, transient analysis is presented in the PCSR for a fault occurring at 102% power with the most onerous single failure, most onerous preventative maintenance and the coincident loss of offsite power all assumed. The 4250 MWth analysis has assumed a partial cooldown rate of 100°C/h. The assessed cases exhibit some core uncovery but the peak clad temperature in the worst case (80 cm^2) only reaches 605°C. The limiting 80 cm^2 case has been repeated at 4500 MWth (with the other assumptions unchanged) for the UK PCSR. The revised assessment predicts core uncovery with a peak cladding temperature of 825°C. Using these results, EDF and AREVA claim that for all the considered IBLOCA and LBLOCA faults the cladding temperature remains below the acceptance criteria of 1200°C, the maximum percentage of total cladding thickness oxidised is less than 17%, there will be no cladding rupture, and the core geometry will be maintained.

173 A second assessment is reported to demonstrate that the safe shutdown state can be reached using only F1A and F1B systems. It consists of a thermal hydraulic transient calculation of the most onerous IB/LBLOCA (the largest cold leg break, i.e. the 390 m^2 SIS line break) with CATHARE coupled with the containment code CONPATE. The reported analysis, which considers the loss two diesel generators through a combination of the worst single failure and preventative maintenance, was actually undertaken for the 4900 MWth reactor design. The PCSR states that the 4900 MWth analysis shows that adequate core cooling is achieved for the SIS line break, and therefore this claim can be made for all IB and LBLOCA identified for a 4500 MWth reactor.

174 IB and LBLOCA faults in shutdown State B are discussed in the PCSR but these have not been assessed in the Step 3 review.

2.3.2.6.6 ND Assessment of Design Basis IBLOCA and LBLOCA Safety Case

175 The design basis analysis for LOCA faults presented in the PCSR appears systematic and thorough.

176 The approach adopted appears to capture and bound all potential LOCA up to the largest pipe connected to the RCS loop. It is for ND's Structural Integrity Inspector to accept break preclusion arguments which would support the claim that a guillotine break of the main RCS pipework is beyond design basis.

177 The fault sequences for the different break sizes are clearly described. The analysis assumes a coincident loss of off-site power and the unavailability of systems due to the limiting single failure and preventative maintenance are considered. The PCSR claims, with supporting transient analysis, that a controlled state can be reached with just automatic F1A systems. Operator actions are required to reach a safe shutdown state and for the larger breaks these can require a significant appreciation by the operator of the situation to ensure the correct actions are followed. While it will be for ND's PSA and Human Factors Inspectors to assess whether these claims are reasonable, they are clearly identified in the design basis and due consideration has been given to the times required for the operators to make these actions.

178 The peak cladding temperature predicted by the limiting calculation 80 cm^2 case is 825°C. Although the PCSR states that this result supports the conclusion that there will be no cladding rupture and the core geometry will be maintained, I do not believe this is definitively the case and no further evidence is provided to backup this claim. However, the analysis has assumed a partial cooldown rate of 100°C/h while it has been confirmed by EDF and AREVA that the planned cooldown rate for the UK EPR is 250°C/h (Ref. 18). Based on the analysis undertaken with a cooldown rate of 200°C/h, EDF and AREVA have estimated the benefit of the proposed UK cooldown rate to be approximately 200ºC to 250ºC on the peak cladding temperature (although core uncovery still occurs).

179 The vulnerability of the EPR design to core uncovery for IBLOCAs is a result of the design choice to go for medium head safety injection as opposed to high head safety injection. It is therefore an area for close scrutiny in the Fault Studies assessment for GDA. The claims and supporting transient analysis presented in the current PCSR (Ref. 1) to demonstrate the acceptability of the LOCA faults are unconvincing. The currently unreported analysis with the higher partial cooldown rate would appear to provide the evidence to make a robust safety case and therefore in Step 4 EDF and AREVA will be asked to formally incorporate the new analysis into their submission.

180 The main code used for the thermal hydraulic assessment of the LOCA faults is CATHARE. Flow of water through the core is represented as two distinct phases: water and steam. The forces and heat transfers between the water, the steam and the reactor components are represented, based on empirical models. The code represents the plant as a series of finite volumes in accordance with general practice and has been used extensively to simulate the response of existing PWR plant. I believe that it meets the requirements of SAP FA.17.

181 The code has been assessed, for its ability to predict the LBLOCA response, against separate-effect and integral test matrices as required by SAP FA.18. These test matrices have been systematically derived and appear to be fit for purpose.

182 The code contains a number of empirical models that are tuned to realistically represent the performance of a set of separate-effect tests. The result being that integral-test performance is generally well represented.

183 I believe that the modelling of dispersed droplet flows is potentially a weakness in current versions of the code, but the model has been tuned to provide a good representation of the rate of quench-front progression in LBLOCA. The fuel peak cladding temperatures tend to be over predicted in some cases. This is an important conservatism for fuel assessment and the effect appears to be sufficiently small not to introduce a significant error in the assessment of containment pressure.

184 The code assessment documents argue that CATHARE can be considered to be best-estimate based on the fact that errors have been determined to lie within the bounds of experimental uncertainty. I believe that this logic is not sufficient to meet the requirements of a best-estimate assessment. SAP FA.18 requires that care should be exercised to take account of uncertainty. Conditions where experimental data lacks precision should not permit reduced requirement for accuracy. I believe that the modelling of core reflood is a particular area of uncertainty that could benefit from some independent assessment as part of Step 4.

185 I have not examined the modelling of the containment for Step 3. This will take place during Step 4. The analysis presented to demonstrate the ability of the design to reach a safe shutdown state from the controlled state, including modelling of the containment behaviour, has not been assessed for Step 3. This will be reviewed in Step 4. Therefore, I am unable to comment at this stage on the appropriateness of the CONPATE code and its use coupled with CATHARE.

186 The offsite dose predicted for a LBLOCA (bounding IB and SBLOCA) is less than 1 mSv. This calculation includes a pessimistic assumption of a cladding failure fraction of 10% despite no core damage being predicted. This would seem to be compatible with the numerical targets in the SAPs (Ref. 4) although the details of the radiological assessment calculations will need to be reviewed in Step 4 in collaboration with ND's Radiological Protection and Chemistry Inspectors.

187 The analysis of intermediate LOCA faults is essential to demonstrate the acceptability of the significant EPR design feature of MHSI. It therefore places sizing requirements on the MHSI pumps. The EPR sizing report (Ref. 20) has not been reviewed in Step 3 but it will be assessed in Step 4 in collaboration with ND's Mechanical Engineering Inspectors. The 80 cm^2 break case would also seem to define a requirement for a partial cooldown rate greater than the 100°C/h assumed in the presented PCSR analysis. This is achieved by the C&I system altering the MSB and MSRT setpoints. The integrity requirements for this procedure will be investigated further in Step 4.

188 LBLOCA effectively sizes the accumulators. The available analysis appears to support the current sizing provided that the break preclusion arguments are accepted, the risk associated with one check valve failing can be tolerated and the detailed review of the analysis is supportive.

189 There is little evidence presented on how the ALARP principle is applied to LOCA faults. Chapter 17 of the PCSR does state that the core is at a lower elevation to the cold leg cross-over piping to limit core uncovery during SBLOCA. The decision to have MHSI pumps with a maximum head below the safety relief valve pressure setpoints on the secondary side has a welcomed benefit for SGTR faults but it is to the detriment of LOCA faults. However, the available transient analysis and dose assessments suggest that there is no significant increase in risk from LOCA faults to compromise the benefit to the risks from SGTR faults.

190 The EPR approach to demonstrate defence-in-depth and the tolerability of the design to common cause failures of safety systems for the more frequent SBLOCA is noted. The analysis presented in the PCSR for the RRC-A LOCA events has not been assessed in detail for Step 3. I intend to return to these sequences in Step 4, particularly considering whether it is appropriate to use non-bounding calculations and make F2 claims for faults which may fall within the SAPs definition of being within the design basis analysis.

2.3.2.6.7 Summary of Requesting Party's Safety Case for 2A-LBLOCA

191 EDF and AREVA make a Break Preclusion argument which excludes consideration of failures of the main primary-circuit pipework from deterministic assessment of the reactor design. It is for ND's Structural Integrity Inspector to accept these arguments. However, an assessment of a double-ended (2A) guillotine failure has been made to demonstrate the capability of the design to withstand the fault and to justify the fault as successfully protected for the purposes of PSA (Ref.21). Nevertheless, the Break Preclusion argument allows the fault to be modelled using less onerous assumptions. Guidance for the assessment of the consequences of a main pipework rupture is provided (Ref. 22).

192 The objective is to demonstrate that a coolable geometry is maintained in the fuel and that the amount of hydrogen released into containment is sufficiently low that this does not present a concern. This transposes directly to ensuring that the cladding surface temperature does not exceed a specified value, but recent analysis has also been able to demonstrate that few if any of the fuel pins would be expected to fail.

193 The release of steam from the reactor into the containment building results in an increase in containment pressure, but the assessment demonstrates that this is within the design capability.

2.3.2.6.8 ND Assessment of 2A-LBLOCA Safety Case

194 I have assessed the available transient analysis of a 2A-LBLOCA 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 and also against SAP KP.2 which requires consideration of severe accidents as part of a strategy of defence in depth.

195 The assessment of the effects of a guillotine fracture of the main primary-circuit pipework is based on an event initiated from normal operating conditions and does not assume any additional failures of protection systems.

196 The cladding temperature reported in Ref. 21 is demonstrated to remain sufficiently low that burst is avoided. This appears to be a significant improvement over current designs, although it must be recognised that the analysis for Sizewell B was not performed on the same best estimate basis. Furthermore, this report (Ref. 21) is not currently part of the PCSR and so it will need to be referenced in the next revision.

197 The analysis considers the fuel as comprising a number of cohorts depending on the level of fuel irradiation. This allows benefit to be claimed for the reduction in fuel pin power as the fuel pin pressure increases with fission gas release.

198 The bounding envelope assumed in the assessment shows little margin to the ratings achieved in the demonstration fuel cycle and could represent a challenging operational constraint in designing future fuel cycles. Attention will need to be given to proposed compliance arrangements when they become available.

199 No assessment of the effect of hydrodynamic forces resulting from the rapid depressurisation has been made. It is conceivable that these forces could result in some damage to vessel internals and distortion of fuel assemblies. This merits further consideration if the fault is to be credited as a success within the PSA.

2.3.2.7 Anticipated Transient without Trip

2.3.2.7.1 Summary of Requesting Party's Safety Case

200 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 1×10^{-3} per year. Such faults are therefore known as anticipated transients. Where such a fault occurs without reactor trip, it is described as an ATWT.

201 EDF and AREVA do not consider ATWT events to be within the design basis of the UK EPR and so no design basis safety case is presented within Chapter 14 of the PCSR. However, they do consider ATWT events within the RRC-A risk reduction sequences. Two possibilities are considered; failure of the control rods to insert following a reactor trip signal and failure of the RPS to initiate a reactor trip signal. The risk reduction feature introduced to protect against failure of the rods is to introduce an ATWT signal that is triggered by the RPS 20 seconds after a reactor trip signal if either the RCCAs are still in the high position or there is a high flux signal. The ATWT signal automatically initiates the EBS and isolates the CVCS. In addition, the ATWT signal ensures that the RCPs are tripped when a low-2 steam generator level signal is received. In the case of the RPS failing to trip the reactor, the Process Automation System (PAS), which EDF and AREVA claim is a diverse system from the RPS, trips the reactor and turbine following receipt of a low 3 steam generator level signal.

202 For those cases which EDF and AREVA consider to be RRC-A sequences, they have performed detailed analyses and demonstrated that even for the most bounding faults

either the RPS or the PAS is able to detect the ATWT event and mitigate the effects sufficiently quickly to prevent DNB, so avoiding significant fuel damage. On the basis of the analysis presented, EDF and AREVA have concluded that adequate protection is provided for the full range of ATWT faults considered.

2.3.2.7.2 ND Assessment

203 In the UK existing relevant good practice is to consider ATWT faults to be within the design basis (Ref. 23) for PWRs. The EDF and AREVA position is therefore considered not to be completely acceptable. 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) and not just the PCC-2 events considered by EDF and AREVA. It is noted that such analysis was performed for Sizewell B (Refs 24 and 25) at the request of HM Nuclear Installations Inspectorate (Ref. 23).

204 In the case of Sizewell B, the design was provided with a diverse emergency boration system to protect against ATWT faults. EDF and AREVA are claiming that the automatic actuation of the EBS 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 reviewed in detail in Step 4 to ensure the requirements of SAP ERC.2 have been met.

205 Within the PCSR, EDF and AREVA have considered the following PCC-2 faults which they consider to be the limiting ATWT precursor events within this RRC-A category:

- excessive increase of secondary side steam flow;
- loss of main feedwater flow
- loss of off-site power to the station auxiliaries;
- uncontrolled boron dilution;
- uncontrolled RCCA bank withdrawal.

206 In addition to these events, Sizewell B (Refs 24 and 25) considered the effects of loss of load, turbine trip, spurious reactor trip and the accidental depressurisation of the primary circuit due to spurious opening of either a pilot operated relief valve or safety valve.

207 In this preliminary assessment performed for Step 3 of the GDA only the design basis analyses (including the relevant RRC-A sequences) have been reviewed using SAPs FA.1 to FA.9. The transient analyses of such faults performed to underpin the success criteria for the PSA have not been examined within Step 3 and so SAPs FA.10 to FA.13 are not discussed. This work will be performed as part of Step 4. To aid my judgement I have benchmarked the analysis approach adopted by EDF and AREVA against some scoping analysis performed in support of the original Sizewell B PCSR (Refs 18 and 19) as an exemplar of relevant good practice in the UK.

208 The EDF and AREVA analyses use the MANTA, SMART, and FLICA III computer codes to model these ATWT transients. The MANTA and SMART codes are used to perform coupled thermal hydraulic and 3D neutronic analysis. As such, the analysis is attempting to perform a realistic calculation of the negative feedback effects associated with any increase core voiding that will occur. The calculations are therefore using essentially best estimate techniques rather than the more traditional point kinetics methods adopted for in the Sizewell B analysis (Refs 24 and 25) which is known to be conservative. 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. I will also commission independent confirmatory analysis for a

selection of the ATWT faults using coupled 3D reactor physics and thermal hydraulic analysis techniques.

209 Although EDF and AREVA aim to perform a best estimate analysis for RRC-A sequences, they do not allow any claims on operator action for 30 minutes within the analysis. Given that ATWT events are relatively fast faults, in practice this means that any protection systems have to be automated meeting the requirements of SAPs ESS.8 and ESS.9. No account is taken of the single failure criterion. However, in my judgement, this still meets the requirements of SAP EDR.4 since common mode failure of the reactor trip and shutdown systems is being considered. The design limits that are being assumed are to avoid pressurising the reactor vessel above 228 Bara and keeping the value of DNBR above 1.21.

210 With regard to the failure of the RCCAs to insert ATWT faults, the analysis shows that although the reactor goes water solid, the flow capacity of the PSVs together with the beneficial effect of the core voiding due to the RCP coast down are sufficient to keep the primary pressure below 187 Bara for the most limiting fault which is the increase in steam flow case. The lowest DNBR is associated with the loss of off-site power case which has a DNBR of 2.36. As with the decrease in reactor coolant system flow rate fault discussed above, I am keen to understand how uncertainties within the DNB correlations have been treated within these best estimate analysis and this will be explored further with EDF and AREVA in Step 4.

211 The ATWT events associated with failure of the RPS to trip the reactor are generally less onerous than those associated with the failure of RCCAs to insert in terms of reactor overpressurisation. However, the minimum DNBRs for the boron dilution and the RCCA bank withdrawal faults at 2.03 and 2.25 respectively, are more limiting. This class of fault does not arise on Sizewell B as it is effectively eliminated by having a diverse SPS that duplicates many of the trip signals provided on the PPS. In contrast, the PAS only trips on low-3 steam generator level and so there is a significant delay before the reactor is tripped compared with the position at Sizewell B. This issue will need to be explored with EDF and AREVA in Step 4 to ensure that the trip signal coverage provided on the PAS is adequate from an ALARP perspective.

212 When comparing the Sizewell B results (Refs 23 and 24) with the UK EPR result, it must be remembered that the Sizewell B results were performed using a very conservative assessment methodology. Sizewell B also considered the following single failures: failure of one of the lines on the emergency boration system, failure of one of the auxiliary feedwater pumps, and failure of one of the steam generator safety relief valves. The associated design limits, a primary pressure of 220 Bara and a DNBR limit of 1.3, are also tighter. With regard to the failure of the RCCAs to insert ATWT faults, the analysis for Sizewell B (Refs 23 and 24) shows that although the reactor goes water solid, the flow capacity of the POSVs and PSRVs, together with the beneficial effect of injecting boron into the circuit using the emergency boration system, is sufficient to keep the primary pressure below 187 Bara for the most limiting fault which is the loss of feed fault. The lowest DNBR value at 1.3 is associated with the loss of off-site power case which is equal to the DNBR design limit. It is very noticeable that the emergency boration system is less effective for the loss of off-site power case because of the associated rundown of the RCPs which minimises the amount of borated water that enters the primary circuit. Given the differences in the analysis assumptions, it is difficult to assess the worth of the emergency boration system at Sizewell B compared with the proposed systems for the UK EPR. In my judgement, in Step 4, EDF and AREVA will need to perform a sensitivity study on the effects of providing an equivalent emergency boration system on the UK EPR to the one of Sizewell B so that an objective ALARP assessment of the benefit of such a system can be made.

213 Within Step 3 no attempt has been made to review the radiological assessments supporting these ATWT fault assessments although it is known that these assessments have been made against the same dose criteria used for PCC-4 events. During Step 4 it will be necessary for such an assessment to be made against the UK requirements given in SAPs FA.3, FA.7 and Target 4 although I judge that any differences are likely to be minor due to methodological assumptions and it is unlikely to require additional protection measures for these faults.

2.3.2.8 Spent Fuel Pool Faults

2.3.2.8.1 Summary of Requesting Party's Safe Case

214 The design of the spent fuel pool racks and cooling system is described in the PCSR. In addition, the requirements for spent fuel cooling are set out in the system design manual (Ref. 26).

215 The main safety criteria for faults in the spent fuel pool are that the fuel remains covered by water while in the racks or while being handled, and that sub-criticality is preserved.

216 The underwater storage racks are designed such that the K_{eff} multiplication factor does not exceed 0.95 in normal operation and 0.98 in credible accident situations even when fuel assemblies with the highest enrichments are considered. Zero boron content in the pool is considered a credible accident.

217 The spent fuel pool purification and cooling system (FPPS / FPCS) is required to remove the decay heat from spent fuel assemblies in the pool. It also contributes to the containment of radioactive substances by ensuring capability for isolation of the fuel building.

218 The FPCS comprises of two identical main trains, each equipped with two pumps and a heat exchanger cooled by the CCWS. The CCWS is cooled by the ESWS. Each train is supplied by a different electrical board and may be supplied by a neighbouring train during electrical switchboard maintenance. The main trains have emergency backup supply from the main diesel generators of each division.

219 The FPCS has a third cooling train equipped with a pump and a heat exchanger cooled by Ultimate Cooling Water System (UCWS). This heat sink is independent of the CCWS / ESWS. This train can also be supplied from an alternative electrical division if its main division is taken out for maintenance. In addition, it is possible to power the third train with the aid of a standby diesel generator.

220 The two main FPCS trains are F1B classified. The third train is F2 classified.

221 The FPCS heat exchange capacity is required to be sufficient to remove the decay heat from the fuel assemblies and prevent boiling, with suitable margins. Nevertheless, the system is required to restart when the spent fuel pool water is at 100°C.

222 During normal operating conditions, a single FPCS train with a single pump operates continuously with the second FPCS train acting as backup. The third train is normally permanently isolated from the spent fuel pool. However, in the event of the main cooling train being unavailable due to preventative maintenance, it is set to start.

223 During unit shutdown, two FPCS trains operate permanently from the start of unloading to the end of reloading. The third train does not operate but is available.

224 The FPPS / FPCS is designed such that a leak or a break will not result in the direct uncovering of fuel stored in the rack, even without any isolation action. Draining through a pipe connected to the pool should not lead to the uncovery of an assembly being handled before the drainage pipe can be isolated or the fuel placed in a safe position. If the drainage leads to a loss of cooling, then emergency makeup is available to avoid the

delayed uncovering (as a result of boiling or evaporation) of fuel in the rack and to re-establish the water level to a height sufficient to allow the restart of at least one train of FPCS. Makeup water is available from the IRWST, Reactor Boron and Water Makeup System (RBWMS), the demineralised water supply and the fire protection systems.

225 The FPCS is designed to meet the single failure criterion, with pump failure and loss of an electrical board considered, and the third train providing some diversity. Isolation of the compartment drainage lines has also been designed to meet the single failure criterion.

226 Design basis spent fuel pool faults are considered in the PCSR (Chapter 14) alongside reactor faults. They are also described in the Fault Schedule. For PCC FPCS faults, the PCSR imposes a temperature limit criteria of 80°C for faults without draining and no boiling for faults involving a fuel pool draining (with the long term temperatures returning to below 80°C once FPCS has been restored). A 95°C limit is applied for RRC-A faults.

227 The loss of one train of FPCS during normal reactor power operation is identified as a PCC-2 design basis transient. Both End Of Cycle (EOC) and Beginning Of Cycle (BOC) FPCS conditions are considered. At EOC, before the shutdown and with the decay heat load in the pool at a minimum, refuelling maintenance of the main FPCS train can be scheduled. At BOC, when the decay heat is higher than any other time during the reactor cycle, maintenance can be performed on a support system (e.g. CCWS). For both cases, it is claimed that the water temperature will not exceed 80°C throughout the transient.

228 A long term loss of offsite power during normal reactor power operation resulting in the loss of the electrical supply to all plant auxiliaries is identified as a PCC-3 design basis incident. Faults occurring at EOC and BOC, with appropriate assumptions on decay heat and maintenance, are considered. It is claimed that EDGs can be utilised to reintroduce the cooling functions before the water temperature reaches 80°C (calculated to take several hours).

229 The loss of one train of FPCS during refuelling is identified as a PCC-3 design basis incident. The last fuel element is assumed to have just been unloaded from the reactor vessel and placed in the spent fuel pool. Two FPCS main trains are assumed to be in service before the fault, with one pump operating per train. One scenario considered is an initiating event of a pump on one of the main FPCS trains failing and the single failure applied to the second pump in the same train. The still operational second train is claimed to be sufficient to keep the water temperature below 80°C. A second scenario is the heat exchanger from one main train being lost. It is argued that a single failure should not be applied to the components of the second main train as it is in operation before the event and remains operational with no change in state required. As before, the second train is claimed to be sufficient to keep the water temperature below 80°C. No claim is made on the third FPCS train.

230 Isolatable piping failures on systems connected to the spent fuel pool (in all reactor operating states) are identified as PCC-3 design basis incidents. For some of the identified pipe failures, the elevation of the pipes or anti-siphon devices prevent the pool water draining to a level where the main FPCS pumps would automatically shutdown. For a piping failure on a skimming line, it is claimed that the operator has sufficient time (1 to 2 hours) following the raising of low level alarms to remove the floating skimming device, reach a controlled state and subsequently reach a safe shutdown state.

231 For failures in the FPCS pipework on the suction side of the pumps, water could drain down beyond the automatic shutdown level of the FPCS pumps. Siphon breakers and / or uncovery of the suction pipe stops the level dropping too low and it is claimed that the breached FPCS train can be isolated using two redundant valves on the suction pipe. Once the break has been isolated, water makeup is undertaken to raise the water level sufficient for a train of the main FPCS to be restarted. The PCSR presents the results for various reactor states and pool fuel loadings showing that the water does not

boil during the transient and that once the cooling has been restored the temperature stabilises to a level below 80°C.

232 An isolatable break in a pipe in the SIS systems (<250 mm diameter) or a non-isolatable break in a line connected to the primary circuit (<50 mm diameter) could result in the drainage from the spent fuel pool if it occurred during cold shutdown with the reactor cavity flooded for refuelling. These faults are identified as PCC-4 design basis accidents. For the isolatable break, it is claimed that the SIS / RHR suction line will be automatically isolated by the closure of two redundant motorised valves upon detection of a low water level in the reactor building transfer compartment. The setpoint for this action is slightly below the level at which the main FPCS pumps will shutdown. However, calculations are presented, which show that the fuel pool water does not boil before makeup water can raise the water level to a position for the main FPCS to restart and maintain the long term temperature below 80°C. Similar analysis is presented for the non-isolatable break but given that the leakage cannot be stopped, it is necessary to provide permanent makeup with the MHSI pumps in recirculation mode between the IRWST and the primary cooling system.

233 It is noted that the PCSR and its supporting reference (Ref. 27) state that the results presented for these faults are only preliminary and could be re-evaluated after the design is finalised.

2.3.2.8.2 ND Assessment

234 The design basis analysis presented in the PCSR and its supporting references is logically and clearly presented. The design criteria are unambiguously stated and the results of analyses are summarised to show how those criteria have been met.

235 Single failures and preventative maintenance have been considered in accordance with the PCSR's stated rules. EDF and AREVA have therefore provided the information to allow an assessment against SAPs FA.6, EDR.2 and EDR.4. However, the loss of one main FPCSs train during refuelling due to a heat exchanger failing is argued to be acceptable, because the second main train is in operation before the event and remains operational with no change in state required. If passive failures before 24 hours have elapsed are considered in addition to active failures (see Section 2.3.2) then additional arguments may be necessary. I recognise that no claim is currently made on the third FPCS train for this fault. If EDF and AREVA are able to demonstrate that this train is capable of acting as a diverse safety system, and that it is qualified to an appropriate standard, then the FPCS probably would be tolerable to such a passive failure.

236 There is in fact little discussion on any safety claims placed on the third FPCS train. Chapter 16 of the PCSR suggests that it has been provided as a RRC-A defence in depth feature to protect against the loss of the two main trains of FPCS (hence the F2 safety classification). However, the current revision of the PCSR does not discuss this fault in detail.

237 The analysis aims to show that the water level will never fall low enough for the fuel in the racks to be uncovered and that FPCS could always be restored (if lost) before boiling could occur. The use of siphon breakers is a specific design feature to restrict the water drain down level. There is a significant claim in the PCSR that the failure of siphon breakers need not be considered, accompanied by some supporting arguments. The arguments seem reasonable and the siphon breaker designs are intrinsically simple but further information will be sought in Step 4 (in collaboration with ND's Mechanical Engineering Inspectors).

238 No complex computer codes have been used in the fault analysis. Instead easily repeatable 'hand calculations' appear to have been used considering volumes, flow rates and specific heat capacities / enthalpy changes. This is entirely appropriate and

assessment against SAPs FA.17 to FA.24 is straightforward. The assumptions made to calculate bounding decay heat levels for the fuel in the pool may be reviewed in Step 4 but this is not expected to be an issue for concern.

239 Other ND Inspectors will take the lead in assessing the design of the spent fuel racks and the criticality evaluation but no specific areas of concern have been identified from a fault studies perspective during Step 3. It will be necessary during Step 4 to be satisfied that the fuel in the racks will remain sub-critical even if the pool water is made up from unborated following a pipe break fault.

240 It is planned in Step 4 to review the identified supporting references (Refs 26 and 27) in more detail and collaborate with other ND colleagues to take a holistic view on the design of the spent fuel pool. EDF and AREVA will be asked to provide details on when the design and therefore the fault analysis will be finalised. Clearly, EDF and AREVA will need to review all frequent design basis faults on the fuel pond in response to the RO requiring that two diverse safety systems, qualified to an appropriate standard, are provided for each safety function.

2.3.2.9 Shutdown Faults

2.3.2.9.1 Summary of Requesting Party's Safety Case

241 In this section I have only considered reactor faults. Spent fuel pool faults have been assessed separately (see Section 2.3.2.8).

242 The design basis analysis of shutdown faults is considered in the PCSR alongside at-power faults. Those faults which occur shortly after shutdown and that have been discussed in the PCSR simultaneously with their at-power equivalents are also not discussed below.

243 Six reactor states, A to F are clearly defined and the faults associated with the appropriate state. States C and D consider operation at a lowered mid-loop RCS level. Described as ¾ loop operation, the arrangement allows the RCS inventory in the plenum and the SG U-tubes to be reduced during plant start-up, and to drain the pressuriser and purge the RPV head with nitrogen before opening to atmosphere. ¾ loop operation also allows the SGs and the RCPs to be maintained.

244 Two PCC-2 faults are identified. The first is uncontrolled RCS level drop in States C and D. The PCSR states that the most probable way this could happen is a fault during the draining of the RCS to ¾ loop. It is argued that such faults bound a SBLOCA in shutdown states C and D.

245 There are four water level instruments, one in each RCS hot leg, dedicated to mid-loop operation. The RCS level is maintained by a loop level control. A reference level is entered and a control system adjusts the letdown flow rate and therefore the RCS level. The level cannot be allowed to drop too low as the provision of residual heat removal by the SIS / RHRS trains could be threatened by vortex formation and cavitation in the suction lines and LHSI pumps. Therefore, the reference level must ensure correct SIS / RHRS operation.

246 In States C and D, 3 SIS / RHRS trains are in operation to remove residual heat. If the loop level controller allows the level to drop beneath the reference level, an operational alarm is generated and an interlock stops further letdown. Ultimately, the MHSI provides automatic safety injection on RCS loop level < MIN. This last signal to start the MHSI is F1A classified.

247 The PCSR states that if an operator error is assumed which results in continuous draining at the maximum inventory loss rate past the reference level, the suction condition limits of the SIS / RHRS could be reached in 9 to 10 minutes. This is stated to be sufficient time

for the MHSI to actuate and inject make-up, even with a single failure of one MHSI train and the unavailability of the second.

248 The failure of the loop level measurement has been identified via PSA as a significant contributor to the frequency of occurrence of an uncontrolled RCS level drop. As a result, the occurrence of the level drop fault without a safety injection signal from the reactor protection system is identified as a RRC-A event. A back-up signal actuating safety injection on a low loop level diverse signal, which does not rely on the same loop level measurements of the protection system, is provided to address this concern.

249 The second PCC-2 event identified is the loss of one cooling train of the SIS / RHRS in residual heat removal mode while in States C or D (with ¾ loop operation). During the considered states, three out of the four SIS / RHRS trains are required to be in operation (with the fourth on standby) to maintain the RCS temperature below 55°C. As with the uncontrolled RCS level drop fault, the concern is to maintain the conditions within the SIS / RHRS suction lines such that residual heat removal is not compromised. Referencing analysis undertaken for a 4900 MWth EPR (Appendix 14B of the PCSR), it is claimed that two SIS / RHRS trains are able to maintain a RCS temperature in a range (< 70°C) which ensures their continuous proper action operation. The start-up of the fourth stand-by train is not claimed in the analysis.

250 The PCSR identifies one PCC-3 shutdown fault (initiating frequency between 1×10^{-4} per year and 1×10^{-2} per year) not associated with the spent fuel pool; the uncontrolled withdrawal of an RCCA bank during States B, C and D. The uncontrolled withdrawal of a RCCA bank during State A is identified and assessed as a PCC-2 event. However, once the reactor leaves State A, a dedicated protection function utilising primary temperature and pressure measurements automatically cuts off the RCCA power supply. The same protection function which cuts the power supply when the temperature or pressure are less than the setpoints, also allows the operator to manually reconnect the power supply once the setpoints are exceeded. The primary temperature and primary pressure measurements used in the permissive derivation are acquired from the Protection System and are F1A classified. As a result of this design feature, the PCSR does not consider the potential PCC-3 shutdown fault further.

251 The long term (between 2 and 24 hours) loss of off-site power in State C is classified in the PCSR as a PCC-4 design basis accident (initiating frequency between 1×10^{-6} per year and 1×10^{-4} per year). The loss of power leads to the temporary loss of decay heat removal via the LHSI / RHR trains and any operational secondary side feedwater supply from the startup and shutdown system. It is claimed that the automatic startup of the EDGs will allow the LHSI / RHR function to be re-established within 40 seconds. In that time, the temperature rise in the RCS water will be only a few degrees.

252 Allowing for the stated most significant single failure (one EDG failing to start resulting in loss of one LHSI / RHR pump and one of two available EFWS pumps) and assuming one LHSI / RHR train is unavailable, it is claimed that the RCS water can be kept below 95°C. State C is sub-divided into normal inventory and low loop level operation. To ensure that the design basis analysis is conservative, the higher permissible decay heat for normal inventory operations is combined with a low loop level reactor inventory. A single LHSI / RHR train available from 40 seconds is predicted to be able to keep the temperature to below 80°C until, on 30 minutes, the standby LHSI / RHR is manually activated. With this second train in service, the temperature will drop.

253 For normal inventory State C faults, the loss of two SIS / RHRS trains can be compensated for by two SGs on standby and their corresponding MSRT setpoints set at a maximum of 5 Bara (the other two SGs are assumed to be on preventative maintenance). Without further EFWS injection, the SG mass inventory is sufficient to provide heat removal for more than 1 hour.

254 The PCSR presents design basis analysis for a SBLOCA (equivalent diameter less than or equal to 20 cm^2) in reactor States C (LHSI / RHR on and RCS closed) and D (LHSI / RHR on and RCS open with fuel in the reactor). These PCC-4 design basis accidents claim the MHSI will provide safety injection and at least one LHSI / RHR train will be able to remove the decay heat from the RCS.

255 The PCSR presents design basis analysis for an isolatable safety injection system break in residual heat removal mode during reactor States C and D. A break could occur inside or outside the containment, leading to a loss in RCS inventory and the discharge of radioactive primary fluid into the containment or safeguards building respectively. The faults are identified as PCC-4 design basis accidents. Early detection is claimed via F1A measurements for breaks outside of the containment, allowing the SIS / RHRS to be isolated by an automatic F1A action. For faults inside the containment, there is no automatic isolation of the affected train and therefore isolation takes place following operator action assumed to occur 30 minutes after the first significant alarm.

2.3.2.9.2 ND Assessment

256 The uncontrolled RCS level drop fault is a frequent fault (an initiating frequency of less than 1 x 10^{-2} per year) for which I would expect to see two diverse safety systems provided for protection. There is a clear claim on the F1A “RCS loop level < MIN” signal initiating safety injection. However, it is not clear from the PCSR if any formal claim is being placed on the earlier operational alarm and letdown interlock, or on any operator with the 9 minutes before the SIS / RHRS suction lines are threatened. It is recognised that RRC approach has identified the failure of the F1A low level protection signal as a potential issue and as a result a diverse low loop level signal has been installed. While the signal is diverse, safety injection is still reliant on the MHSI. I intend to pursue these issues further in Step 4, initially through TQs.

257 Despite this concern above, the fact that the initiation of the MHSI is automatic is a welcomed improvement on Sizewell B which relies on the operator diagnosing and mitigating the fault (Ref. 31).

258 I have not identified any areas of concern in the narrowly defined fault of a loss of one cooling train of the SIS / RHRS in residual heat removal mode while in States C or D.

259 The arguments presented as to why an uncontrolled withdrawal of a RCCA bank fault during States B, C and D does not need to be considered in the PCSR have not been assessed in detail for Step 3.

260 The tolerance of the EPR design to a long-term loss of off-site power during State C appears to be adequately demonstrated providing the claim that this is a PCC-4 event can be substantiated. The analysis is conservative, combining the higher decay heat of normal inventory operation with an assessment of the temperature rise for low loop operation. Single failures and preventative maintenance have been considered. It is noted that with a full inventory the MSRTs are capable of removing decay heat for at least an hour although it would appear that this is neither needed nor claimed for the design basis analysis. It is not clear whether the upper limit on recovery time of 24 hours is an arbitrary cut-off or associated with any claim that something can be achieved in that time. I intend to pursue these issues further in Step 4, initially through TQ’s.

261 The design basis analyses for a SBLOCA in reactor States C and D and for an isolatable safety injection system break in residual heat removal mode have not been assessed in Step 3.

2.3.2.10 Heterogeneous Boron Dilution Faults

2.3.2.10.1 Summary of Requesting Party's Safety Case

262 Heterogeneous boron dilution events are characterised by the formation of an unborated slug in a loop of the RCS while the boron concentration in the rest of the RCS is unchanged. The dilution can be external in origin, i.e. water of low or zero boron concentration is injected into the RCS, or intrinsic as a result of certain accident conditions, e.g. reflux condensation during a SBLOCA. EDF and AREVA claim that heterogeneous slug formation cannot occur when the RCPs are running as the flow will be sufficient to mix the unborated water with the borated water. Once formed, the risk is that the slug could be transported to and through the core (e.g. by the restarting of the RCPs) resulting in a reactivity insertion.

263 Heterogeneous boron dilution faults are not considered explicitly amongst the design basis faults discussed in Chapter 14 of the PCSR. However, they are considered in the PSA section (Chapter 15) and in Chapter 16.3 on Practically Eliminated Situations (defined as situations where the implementation of specific design measures have been made to reduce the risk of a large early release of radioactive material to the environment to an insignificant level). No safety case is presented for intrinsic faults.

264 It is claimed that the largest slug which could be formed by inadvertent CVCS injection during isolation of makeup is limited to 2 m^3 because of F1A boron meters installed on the main CVCS injection line. The suction lines on the CVCS are automatically isolated following a signal from the boron meters, switching over to the borated IRWST. Separately, the heat exchangers cooled by the CCWS system are monitored to detect and to localise potential leaks during normal operation to prevent the formation of a pure water slug in the auxiliary systems connected via the pump seal cooling devices.

265 The maximum possible slug is assumed to be 4 m^3 which corresponds to the total volume of either the cold leg or the total volume in the loop seal.

266 Analysis undertaken with the Computational Fluid Dynamics (CFD) code STAR-CD has been reported (Ref. 28). It shows that a 2 m^3 slug will result in a minimum boron concentration well above the critical boron concentrations identified for the proposed EPR fuel management schemes. A 4 m^3 slug was found to have a volume close to the critical concentration. As a result, this volume was chosen as the 'critical plug size' for PSA assessment.

267 The PSA analysis (Ref. 29) calculated the probability of scenarios leading to a slug larger than 4 m^3 to be 5.2×10^{-9} per reactor year. On that basis, fast reactivity accidents as a result of heterogeneous boron dilution are argued to be practically eliminated.

2.3.2.10.2 ND Assessment

268 The safety case for heterogeneous boron dilution requires both further development and assessment in Step 4. In particular, the technical justification for the estimated initiating frequency will need to be reviewed with the aid of ND's PSA specialists.

269 Currently no safety case is presented at all for intrinsic fault induced dilutions.

270 The determination of the critical plug size is reliant on CFD analysis. This is a methodology which is often sensitive to the skill of the analyst and also requires careful and appropriate validation. This analysis will need to be carefully reviewed during Step 4 and is a priority area for confirmatory analysis by Technical Support Contractors commissioned by ND.

271 The PSA analysis will need to be reviewed against SAPs FA.10 to FA.14 in co-operation with ND's PSA Inspectors.

272 Until this additional assessment is complete, it is not possible to say if the claim that the faults are practically eliminated can be supported or if all measures have been taken to reduce the consequences of this fault in accordance with ALARP.

2.3.2.11 Internal Hazards

273 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.

2.3.2.12 External Hazards

274 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

275 An early failure of the containment in a severe accident would have major consequences (in terms of radiological dose) for the public. EDF and AREVA claim that this is practically eliminated by engineered safety features that concern the following phenomena:

- preventing core melt under high pressure conditions and hence avoiding direct containment heating by the melt;
- avoiding large steam explosions which can threaten the containment;
- limiting hydrogen combustion.

276 A further, equally important objective is the preservation of the containment integrity in the long term by maintaining containment cooling and hence limiting loads on the structure. This is achieved by appropriately engineered systems.

277 The strategy adopted in the case of core melt, is to ensure that the reactor is depressurised and to capture any core melt in a dry reactor pit where sacrificial concrete is used to modify its composition prior to its dispersal and quench.

278 Depressurisation of the reactor is provided by a dedicated diverse system initiated by the operator in the event of a severe accident.

279 Melt stabilisation is provided by spreading the molten core over a core catcher located adjacent to the reactor pit; increasing the surface / volume ratio of the melt.

280 The hydrogen control system of the EPR makes use of a staged approach targeting the following goals:

- the prevention of fast combustion that might challenge the containment integrity;
- a sustained reduction of hydrogen concentration below flammability limits.

281 Rupture and convection foils, as well as hydrogen mixing dampers, normally separate the two zones of the containment, but in the event of a steam release to the containment, these open to promote mixing of the containment atmosphere, limiting local hydrogen concentrations.

282 The possibility of a hydrogen combustion risk in the long-term is avoided by installing autocatalytic re-combiners at appropriate locations in the containment. These maintain the hydrogen concentration below the flammability limit of 4% during the first 12 hours of a severe accident.

283 The containment heat removal is designed to meet a grace period of 12 hours, during which time no active measures for containment heat removal are necessary. For long-term decay heat removal, the EPR has a dedicated containment heat removal system.

2.3.3.2 ND Assessment

284 I have assessed the Severe Accident analysis principally against SAP 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. 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. This also applies to the assessment of severe accident guidance to operators.

285 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.

286 The EPR design addresses severe accidents in a systematic manner. Fault sequences beyond the design basis which have a potential to lead to a severe accident have been identified and results of the PSA have been employed to determine which sequences merit detailed consideration. The results are presented in Chapter 16 of the PCSR, but detailed supporting material needs to be extended to include sufficient of the technical material to allow a future licensee to fully understand the detail of the supporting analysis and if necessary repeat it.

287 In order to demonstrate that there is no cliff edge in terms of fault consequences, it is generally necessary to demonstrate that faults, which could lead to an early large release of fission products to the environment, do not make a disproportionately large contribution to risk. Generally this is demonstrated by showing that containment integrity is maintained for an extended period.

288 The strategy for containing severe accidents has a number of components:

- Vessel depressurisation.
- Hydrogen mixing and oxidation.
- Melt spreading and cooling.
- Containment heat removal.

289 These functions are provided largely by passive systems in accordance with SAP EKP.5 and a degree of redundancy is provided. A large body of research has been carried out in recent years and EDF and AREVA have taken this into consideration as required by SAP FA.15. The key topics are discussed in turn below.

Vessel Depressurisation

290 A failure of the reactor vessel at high pressure is a significant potential contributor to the risk of early containment failure because it has the potential to damage the containment structure by missiles and by direct heat transfer from molten material. Hence rupture of the RCS at high pressure must be excluded by design as far as reasonably practical. For the EPR, this is achieved through two dedicated severe accident depressurisation valve

trains that are part of the Primary Depressurisation System (PDS) but independent of the pressuriser safety valves. The safety valves will potentially be available as a diverse means. The coolant is discharged into the Pressuriser Relief Tank (PRT), which itself is protected by rupture disks which discharge into containment. The system is manually operated and the intention is to activate one train only on demand in order to limit the rate at which reflooding by the accumulators could cause vessel pressurisation and hydrogen release.

291 The operator may depressurise at various stages during a fault but depressurisation will eventually be activated by the operator when the core outlet temperature reaches 650°C. This introduces a degree of uncertainty into the time and rate of depressurisation and introduces the possibility of the accumulator supplying water to hot fuel and causing rapid zirconium oxidation, which potentially results in high rates of hydrogen generation. The impact of this on containment integrity has been assessed by EDF and AREVA and found to be satisfactory. I will consider the approach further in Step 4. In particular, the decision to opt for a manual system will be examined.

292 Pressurised severe accidents also introduce the possibility of bypassing the containment by SG tube failures. EDF and AREVA argue that creep rupture would occur at the weakest point of the primary system. Studies have shown that the weakest point is the bimetallic weld of the hot leg (with no risk of containment by-pass). I will review the evidence supporting this claim in Step 4.

Hydrogen Mixing and Oxidation

293 The hydrogen control system uses 47 re-combiners; sited to limit the effect of high gas temperatures in the exhaust from the units. These units are sized to control the containment mean hydrogen concentration.

294 In the short term, a high hydrogen release rate leads temporarily to a non-uniform hydrogen distribution with high peak concentrations. This unfavourably affects both the possibility for flame acceleration and detonation.

295 Flame acceleration can only occur if the change in density across a flame front exceeds a threshold value. A threshold assessment criterion has been derived directly from experiments and provides an indication of a possible concern. However, EDF and AREVA's analysis indicates that the criterion can be violated locally during the course of a severe accident. In this case, the process of combustion has been explicitly calculated using a special purpose CFD code. This analysis demonstrated acceptable loads on the containment shell. However, I feel that this approach is possibly indicative of small safety margins. I will review the basis of this analysis and the associated validation in Step 4 and will also consider the issue of common-mode failure of re-combiner catalysts.

Melt spreading and cooling

296 The EPR vessel has been designed to remove penetrations for instrument tubes from the lower regions of the vessel and therefore the vessel is more robust against core melt. However, I believe that the power output of the EPR makes in-vessel melt retention by external cooling impractical and EDF and AREVA have opted to retain a dry vessel cavity to limit the risk of steam explosions.

297 The most likely mode of vessel failure (following depressurised molten core relocation) is melt through the side of the vessel followed by creep collapse. Prototypic experiments designed to simulate this type of scenario indicate that the melt would be substantially contained in the vessel pit region where structural concrete is protected from significant thermal damage by a ceramic membrane.

298 While the melt is contained in the pit region, it ablates a layer of sacrificial concrete before leaving the pit and spreading over an engineered 'core catcher'.

299 The core catcher is designed to contain the melt and prevent thermo-chemical damage to the containment concrete base mat. The design includes a number of novel features. A sacrificial concrete layer is designed to oxidise any remaining zirconium metal and to reduce the density of the oxide melt. This strategy is designed to enable the oxide layer to float above a molten metal layer with the benefit that an oxide crust is less able to effectively insulate the upper surface of the melt than a metal crust and therefore over-flooding of the melt will be more effective in removing heat.

300 Below the sacrificial concrete is a sacrificial iron layer over high-temperature refractory tiles. The iron is intended to melt and to isolate the refractory from potential thermal shock or chemical attack.

301 Finally a network of cooling water passages provides a means of freezing the melt in the long term. The system appears to be designed in such a way that the cooling flow is insensitive to minor defects in the bed of the core catcher.

302 The efficient functioning of the core catcher is dependent on ensuring an even spread of melt in the spreading room. This requires that the corium is fully melted at the time of spreading.

303 Late reflooding (around the time of vessel failure) is argued to delay core relocation, but not to change the fault progression significantly because the melt forms a crust that isolates it from the coolant. I have not yet seen detailed analysis to support this claim for a spectrum of scenarios and I suspect that reflooding around the time of melt relocation may have a significant conditional probability. This will be examined in more detail in Step 4 where the effect of uncertainties in the fault progression will be considered.

304 The sacrificial concrete in the vessel pit is designed to give the melt suitable viscosity to spread effectively and when combined with that on the upper surface of the core catcher, is expected to oxidise the zirconium and modify the density of the oxidic melt to ensure a friable crust on the corium upper surface.

305 The chemistry of these processes is novel and has been optimised as part of the containment design (Ref. 30). The design of the core catcher has undergone a process of development in consultation with IRSN. I take comfort from the apparent rigor of the process. I will give the chemical and thermal aspects of the design further scrutiny in Step 4.

Containment Performance

306 Leak tightness of the containment is secured by a steel liner and penetrations designed to withstand ambient conditions prevailing inside the containment in severe accidents. Most leakage is collected in the containment annulus, which is kept at sub-atmospheric pressure by the annulus ventilation system. In the event that leakages are not collected in the annulus, the gas enters the peripheral buildings and where it is also filtered before being released. The design is intended to reduce potential uncontrolled radiological releases from containment to a very low level. I am impressed with the functional capability of the system. It appears to have the required redundancy and diversity, but I am conscious of its complexity and the need for attention to construction and maintenance arrangements.

307 The containment heat removal is principally via spray systems. These are activated manually at the latest 12 hours into a severe accident to reduce containment pressure and temperature below the long-term capability of the shell. One out of two trains is sufficient. A positive side-effect of spraying is scrubbing of particulate releases from the containment atmosphere.

308 The spray water flows back into the IRWST and is chilled and recycled. At the same time, the core catcher is cooled with water flowing passively from the IRWST.

Arrangements are in place to ensure the continued function of the containment cooling systems in the medium term.

309 By design, there is no facility to vent the containment and therefore provide a passive and diverse method of pressure control. This could merit consideration as an ALARP study. I will consider this further in Step 4.

2.3.4 Review of Step 2 Findings

310 The Step 2 Fault Studies assessment (Ref. 5) of the EDF and AREVA UK EPR PSR identified a number of technical issues which ND would need to consider 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 UK EPR technical specifications and the need to validate computer codes.

2.3.5 Use of Overseas Regulators Information

311 An initial meeting has been held with the United States Nuclear Regulatory Commission (US NRC) to share assessment findings on the fault analysis aspects of the UK EPR. Further meetings are planned including attendance at the OECD Multi-national Design Evaluation Programme (MDEP) meetings for the EPR in the fault analysis area. A single MDEP meeting on the severe accident aspects of the UK EPR has already taken place focusing on hydrogen production in containment. 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

312 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.
- The Sandia Fuel Project (SFP) looking into the consequences of severe loss of cooling accidents on a PWR spent fuel ponds.

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

2.3.7 Regulatory Observations (ROs)

314 No Regulatory Observations (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 initiating events in the PSA.

ii) There is a need for EDF and AREVA 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.

iii) There is a need to demonstrate that the fuel is protected from PCI failure for frequent faults.

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

2.3.8 Plans for Step 4

316 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 EDF and AREVA's Fault Schedule for the UK EPR;
- assess the thermal hydraulic analysis undertaken to support PSA success criteria;
- assess the appropriateness and validity of the computer codes used in accordance with SAPs FA.17 to FA.24;
- assess the response to the Regulatory Observations identified above;
- commission Technical Support Contractors to undertake independent confirmatory analysis of selected UK EPR transients.

3 CONCLUSIONS AND RECOMMENDATIONS

317 In general, the range of faults considered within the PCSR is less comprehensive than might be desired. Nevertheless, it is adequate in my judgement to enable a characterisation of the fault conditions on the UK EPR 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.

318 Notwithstanding these reservations regarding the form and completeness of the safety case, there are no fundamental reasons for believing from a Fault Studies perspective that a satisfactory safety case for UK EPR 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 either the reactor protection system (a major change has already been proposed but came too late to be taken into

account in this report) or the qualification of safety systems to an appropriate 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 and can be reconciled with the list of initiating events in the PSA.
- There is a need for EDF and AREVA 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.
- EDF and AREVA will need to describe what are the limits and conditions they are proposing for the fuel safety technical specifications.
- There is a need to demonstrate that the fuel is protected from PCI failure for frequent faults.
- The response to loss of coolant accidents is generally to shut down the reactor and initiate a partial cooldown via the secondary side. The rate of cooldown identified for the UK EPR is 250°C/h but the majority of the transient analysis presented has assumed 100°C/h. There is a need for EDF and AREVA to provide more analysis at the planned cooldown rate for the UK EPR to demonstrate the adequacy of medium head safety injection for the relevant range of loss of coolant accidents.
- ATWT faults need to be included within the design basis. An ALARP justification for not installing an emergency boration system similar to the one installed on Sizewell B will also be required.
- There is a need for EDF and AREVA to demonstrate their safety case for heterogeneous boron dilution beyond what is discussed in the PCSR.

319 It is recommended that these findings, which include the three proposed ROs identified in Section 2.3.7, are formally raised with EDF and AREVA 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 *UK EPR Pre-Construction Safety Report* UK EPR-0002-132 Issue 02 EDF and AREVA June 2009.

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

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

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

5 *Step 2 Fault Analysis Assessment of the EDF and AREVA submission for the UK EPR*, AR 2007/17, March 2008, TRIM Ref. 2008/135506.

6 *UK EPR Fundamental Safety Overview, EDF and AREVA, 2007.*

7 *Step 3 Fuel Design Assessment of the EDF and AREVA UK EPR*, AR 09/040, November 2009, TRIM Ref. 2009/343221.

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

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

10 *Single Failure Criterion*, SECY-77-439, US NRC, August 1977.

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

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

13 *Transient Analysis to support the Generic Safety Case for Sizewell B*, C5166/TR/137, NNC, July 1998.

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

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

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

17 *EPR FA3 Preliminary Safety Analysis Report*, Edition 2003, EDF.

18 *ND GDA Technical Query TQ-EPR-373*, September 2009, TRIM Ref. 2009/308854.

19 *ND GDA Technical Query TQ-EPR-230*, July 2009, TRIM Ref. 2009/244145.

20 *EPR sizing at 4500MWth*. EPRR DC 1685 Revision C. AREVA. February 2002. (E).

21 *Cathare 2A-LB LOCA realistic evaluation model SN/98-00660*, TR 98/71 (E)

22 *Large Break LOCA Design Guidelines*, EDF TR96/50 (1997).

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

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

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

26 *Dossier de Système Élémentaire PTR, P2 – Fonctionnement du système* [System Design Manual Spent Fuel Cooling and Purification System (PTR [FPPS/FPCS]), P2 – System operation], SFL–EFMF 2006.712 Revision G, Sofinel, October 2008.

27 *Etude fonctionnelle relative au traitement des PCC de perte de refroidissement et de vidange des piscines* [Operational study relative to the treatment of the PCC of loss of cooling and draining of the pools]. ECEF080499 Revision A, EDF, April 2008.

28 *Heterogeneous Dilution: Critical Plug Size*. NGES1/2002/en/0241 Revision. D. AREVA. November 2003. (E).

29 *Heterogeneous Boron Dilution – PSA demonstration of dilution accident practical elimination*. NGPS4/2003/en/0120, Revision B, AREVA. 2003. (E).

30 *Severe accidents - improved spreading concept*, SN/96-0952, TR 96/31 (E).

31 *Sizewell B Power Station, Station Safety Report, IR15.5(2) Transient Analyses Of Bounding Limiting Design Basis Faults*, SXB-IP-772001-822, British Energy, November 2008.

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

Table 1

Summary of Relevant Safety Assessment Principles and the Assessment of the EPR against them

SAP	Description	Comment
Fault Analysis		
FA.1 to FA.3	General	The accident analyses performed by EDF and AREVA in Chapter 14 of the PCSR 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 EDF and AREVA in Chapter 14 of the PCSR are assessed against these SAPs in Sections 2.3.2.1 to 2.3.2.12 of this report. The faults considered are cooldown faults, heat-up faults, flow reduction faults, reactivity faults, increase in coolant faults, loss of coolant faults (including SGTR, SBLOCA, IBLOCA & LBLOCA), ATWT faults, heterogeneous boron dilution 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 EDF and AREVA in support of the EPR 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	The methodologies used by EDF and AREVA to calculate the radiological consequences of design basis faults will be assess in Step 4 to allow a meaningful comparison against 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

SAP	Description	Comment
		identified in SAP EK.5.
EDR.1 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.9	Safety Systems	The reactor protection system is assessed against SAPs ESS.2, 4, 6, 7 in Section 2.3.2.4. SAPs ESS.8 is discussed in Sections 2.3.2.2 and 2.3.2.7. ESS.9 is discussed in Section 2.3.2.7.
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.

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-UKEPR-040	11 Nov 2009	Demonstration that the list of design basis faults is complete including shutdown and spent fuel pond faults and can be reconciled with the list of faults identified in the PSA.	New RO to be raised.	Step 4
RO-UKEPR-041	11 Nov 2009	Review all design basis faults with a frequency greater than 1×10^{-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 needs to be extended to included passive failures.	New RO to be raised.	Step 4
RO-UKEPR-042	11 Nov 2009	There is a need to demonstrate that the fuel is protected against PCI failure for frequent faults.	New RO to be raised.	Step 4