Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-020a
Revision 0
21 November 2011

COPYRIGHT

First published December 2011

PREFACE

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

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

EXECUTIVE SUMMARY

This report presents the findings of the Fault Studies assessment of the design basis analyses for the UK EPR reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the November 2009 version of the Pre-construction Safety Report (PCSR) and the supporting documentation submitted by EDF and AREVA during Step 4.

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

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

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

My assessment has focussed on:

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

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

The design basis thermal hydraulic analysis of the containment building during fault conditions, such as a large break loss of coolant accident or a main steam line break, are also reported separately. The assessment of the severe accident analyses performed by EDF and AREVA is covered in the same report as the containment analysis and is therefore also not discussed in any detail in this report.

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

the detailed design of the control and limitation functions within the reactor control, surveillance and limitation (RCSL) system will be specified by the future UK EPR operator and so it has been agreed that these functions are also outside the scope of this GDA Fault Studies Assessment.

In some areas there has been a lack of detailed information which has limited the extent of my assessment. As a result ND will need additional information to underpin my judgements and conclusions and these are identified as Assessment Findings to be carried forward as normal regulatory business. These are listed in Annex 1. Some of the findings identified within this report are of particular significance and will require resolution before HSE would agree to the commencement of nuclear safety-related construction of a UK EPR reactor in the UK. These are identified in this report as GDA Issues (see Annex 2).

From my assessment, I have concluded that:

- EDF and AREVA have undertaken a large amount of analysis work within the Fault Studies assessment area during GDA Step 4 and have made very significant progress against the issues identified in my GDA Step 3 Assessment Report.
- In my opinion, EDF and AREVA have considerably strengthened the design basis safety case for the UK EPR through the additional analysis performed in response to the Regulatory Observations raised in my GDA Step 3 Assessment Report. They have performed a large number of additional sensitivity studies and have demonstrated that the design is particularly well protected against passive single failures. They have also been able to extend the design basis to cover complex situations in which a combination of events may initiate a fault sequence, although this is an area where there is still some further work to be done by the RP and a GDA Issue has been raised.
- The analytical work performed by EDF and AREVA has been aided by a number of important design changes to the Control and Instrumentation (C&I) systems on the UK EPR that in my opinion will significantly improve the safety of the design. These changes have been proactively identified by EDF and AREVA. The design changes identified are:
  - An increase in the partial cooldown rate from 100°C/hr to 250°C/hr following a loss of coolant accident. This has considerably increased the margin of safety on the clad melt temperature limits for the loss of coolant accidents that EDF and AREVA consider to be within the design basis of the UK EPR.
  - Addition of a high neutron flux trip signal and a high axial offset trip signal on one of the diverse reactor protection systems to improve protection against reactivity faults occurring together with a failure of the main reactor protection system.
  - Addition of a high hot leg pressure trip signal on one of the diverse reactor protection systems to improve the protection against loss of normal feedwater faults occurring together with a failure of the main reactor protection system.
  - Addition of a low Reactor Coolant Pump speed trip signal on one of the diverse reactor protection systems to improve the protection against reduction in flow faults occurring together with a failure of the main reactor protection system.
  - Addition of an automatic actuation signal to start the emergency feedwater system using a low steam generator water level signal on a diverse reactor protection system to improve protection against loss of main feedwater faults occurring together with a failure of the main reactor protection system.
  - An improvement to the integrity and detection capability of the activity detectors on the secondary side steam lines to provide better protection against steam generator tube rupture faults.

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

- EDF and AREVA to provide a safety case for heterogeneous boron dilution events covering both intrinsic and external sources of diluted water.
- EDF and AREVA to implement modifications to the reactor protection system and provide further analysis to ensure the provision of functional diversity for faults with an initiating frequency greater than 1×10^{-3} per year.
- EDF and AREVA to provide an updated safety case for the spent fuel pool incorporating faults associated with the cask loading pit.
- EDF and AREVA to provide a revised safety case for steam generator single tube rupture faults to incorporate design changes to the protection for these faults.
- EDF and AREVA to provide a design basis analysis of failures in the essential support systems on the UK EPR.

In my judgement, any additional design changes resulting from these GDA Issues will be limited to the C&I systems. The one exception could be the last issue because the design basis assessment could result in changes to the categorisation and classification of systems that protect against the loss of essential support systems. Nevertheless, in my opinion, it is now highly unlikely that there will be a need for any significant changes to plant layout or the addition of any new safety systems to UK EPR design from a Fault Studies perspective.

Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK EPR reactor design. The UK EPR reactor is therefore suitable for construction in the UK, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

LIST OF ABBREVIATIONS

ALARP	As Low as Reasonably Practicable
AC	Alternating Current
AO	Axial Offset
ASN	Autorité de Sûreté Nucléaire (French nuclear safety authority)
ATWT	Anticipated Transient without Trip
BMS	(Nuclear Directorate) Business Management System
BOC	Beginning of Cycle
C&I	Control and Instrumentation
CAMP	Code and Maintenance Programme
CCWS	Reactor Component Cooling Water System
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
CHF	Critical Heat Flux
CHRS	Containment Heat Removal System
CMF	Change Management Form
CSARP	Cooperative Severe Accident Research Programme
CSNI	Committee on Safety of Nuclear Installations
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
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System
EOC	End of Cycle
ESWS	Essential Service Water System
$F_{\Delta H}$	Total Enthalpy Rise Hot Channel Factor (Radial Power Distribution)
FPCS	Spent Fuel Pool Cooling System
FPPS	Spent Fuel Pool Purification System
GDA	Generic Design Assessment
GRS	Gesellschaft für Aglagen und Reaktorsicherheit mbH
HHSI	High Head Safety Injection
HIC	High Integrity Component
HSE	The Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning

LIST OF ABBREVIATIONS

IAEA	The International Atomic Energy Agency
IBLOCA	Intermediate Break Loss of Coolant Accident
IRWST	In-containment Refuelling Water Storage Tank
ISL	Information Systems Laboratories, Inc
LBLOCA	Large Break Loss of Coolant Accident
LCO	Limiting Condition of Operation
LHSI	Low Head Safety Injection
LLSF	Lower Level Safety Function
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
MDEP	Multinational Design Evaluation Programme
MFWS	Main Feedwater System
MHSI	Medium Head Safety Injection
MOX	Mixed Oxide Fuel
MSB	Main Steam Bypass (to Condenser)
MSL	Master Submission List
MSIV	Main Steam Isolation Valve
MSRCV	Main Steam Relief Control Valve
MSRT	Main Steam Relief Train
MSSV	Main Steam Safety Valves
NCSS	Non-computer based safety system
ND	The (HSE) Nuclear Directorate
NEA	Nuclear Energy Agency
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
PIRT	Phenomenon Identification and Ranking Table
PLSF	Plant Level Safety Function
PPS	Primary Protection System
PSA	Probabilistic Safety Analysis
PSAR	Preliminary Safety Analysis Report
PSRV	Pressuriser Safety Relief Valves (Sizewell B)
PSV	Pressuriser Safety Relief Valve (UK EPR)

LIST OF ABBREVIATIONS

PWR	Pressurised Water Reactor
RAPFE	Radial Averaged Peak Fuel Enthalpy
RBWMS	Reactor Boron and Water Makeup System
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RCSL	Reactor control, surveillance and limitation
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RO	Regulatory Observation
RPS	Reactor Protection System
RRC	Risk Reduction Category
SABL	Safety Analysis Bounding Limits
SAP	Safety Assessment Principles
SAS	Safety Automation System
SBLOCA	Small Break Loss of Coolant Accident
SBO	Station Blackout
SFG	Safety Functional Group
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection System
SPS	Secondary Protection System
SSC	System, Structure and Component
STUK	Säteilyturvakeskus (Finnish Radiation and Nuclear Safety Authority)
TQ	Technical Query
TSC	Technical Support Contractor
UCWS	Ultimate Cooling Water System
US NRC	United States Nuclear Regulatory Commission

TABLE OF CONTENTS

Annexes

1 INTRODUCTION

1 This report presents the findings of the Fault Studies Assessment of the design basis analyses for the UK EPR reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the November 2009 version of the Pre-construction Safety Report (PCSR), Ref. 12, and supporting documentation provided by EDF and AREVA during GDA Step 4. Assessment was undertaken of the PCSR and the supporting evidentiary information derived from the Master Submission List (MSL), Ref. 13. The approach taken was to assess the principal submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Submission Master List on a sampling basis in accordance with the requirements of ND Business Management System (BMS) procedure AST/001 (Ref. 2). The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

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

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

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

2.1 Assessment Plan

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

2.2 Standards and Criteria

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

2.3 Assessment Scope

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

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

8 It should be noted that the assessment of the fuel and core design, which is a technical area that is closely related to Fault Studies, is not reported here but in a separate report (Ref. 15). As a result, the justification of the fuel safety limits during accident conditions, including assessment of the critical heat flux correlations needed to demonstrate fuel integrity during many of the fault transients are not discussed in detail in this report.

9 The design basis thermal hydraulic analysis of the containment building during fault conditions, such as a large break loss of coolant accident or a main steam line break, are also reported separately (Ref. 16). The assessment of the severe accident analyses

performed by EDF and AREVA is also covered by the same report and is therefore not discussed in any detail in this report. The assessment of the Probabilistic Safety Analysis (PSA) is also reported separately (Ref. 18).

10 The principal document considered in the fault study assessment area is the November 2009 Submission of the PCSR (Ref. 12) reflecting the UK EPR design freeze at the end of 2008. Chapters 14 and 16 are the main sections of relevance to Fault Studies. Chapter 6.2 on containment loads and Chapter 3.4 on overpressure protections are also relevant to Fault Studies assessment area. These chapters are not significantly different from the earlier revisions which were assessed in GDA Step 3 and it was through this earlier work that the areas for specific focus in GDA Step 4 were identified. It was also through the work done in GDA Step 3 that the areas for independent analysis by TSCs were identified.

11 In addition to the PCSR, the responses to ROs and TQs received during GDA Step 4 have been subject to detailed assessment. The responses to ROs and some TQs have been reflected in the revised March 2011 submission of the PCSR (Ref. 14). Therefore, some aspects of this latest version of the PCSR will have been assessed in GDA but it is only the November 2009 version of the PCSR (Ref. 12) that has been formally subject to assessment. When the PCSR is referred to in this report, it is Ref. 12 unless otherwise stated.

2.3.1 Findings from GDA Step 3

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

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

14 Specific findings included:

- EDF and AREVA were requested to demonstrate that the list of design basis initiating events was complete and could be reconciled with the list of initiating events in the PSA (RO-UKEPR-40).
- EDF and AREVA were requested 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 needed to be extended to include passive failures (RO-UKEPR-41).
- EDF and AREVA were requested to demonstrate that the fuel is protected from pellet-clad interaction (PCI) failure for frequent faults (RO-UKEPR-42).
- The response to smaller 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 in the PCSR has assumed 100°C/h. EDF and AREVA were requested to provide more analysis at the revised cooldown rate for the UK EPR to demonstrate the adequacy of medium head safety injection for the relevant range of loss of coolant accidents (RO-UKEPR-57).

- EDF and AREVA were requested to perform additional transient analysis sensitivity studies for the cooldown fault analysis studies presented in the PCSR including the steamline break fault (RO-UKEPR-63).
- EDF and AREVA were requested to include Anticipated Transient without Trip (ATWT) faults within the design basis. Specifically, EDF and AREVA were requested to provide technical justification for not installing a fast acting emergency boration system (RO-UKEPR-64).
- EDF and AREVA were requested to demonstrate their safety case for heterogeneous boron dilution faults (RO-UKEPR-65).
- EDF and AREVA were asked to identify what are the limits and conditions for the fuel safety technical specifications (RO-UKEPR-72).

15 These significant findings were captured as ROs for which EDF and AREVA have undertaken additional work and submitted additional documentation during GDA Step 4. These findings have been specific areas of focus within GDA Step 4 and are discussed in this report with the exceptions of RO-UKEPR-42 and RO-UKEPR-72 which are discussed in the Fuel and Core Assessment Report (Ref. 15). EDF and AREVA have consolidated the response to RO-UKEPR-64 on ATWT faults within the response provided for RO-UKEPR-41.

16 During the course of the GDA Step 4 Assessment, it was established that the submitted spent fuel pool safety case did not include fuel despatch through the cask loading pit. This was identified as an additional RO (RO-UKEPR-75) and an initial assessment has been performed.

2.3.2 Additional Areas for Step 4 Assessment

17 Additional areas for further investigation for GDA Step 4 were identified in the assessment plan. These areas have been assessed using already available safety submissions (principally Ref. 12 and its supporting references), the responses to TQs raised during GDA Step 4 and through technical discussions held with EDF and AREVA. In particular, the assessment plan identified five areas that were not assessed during GDA Step 3 that needed to be assessed during GDA Step 4:

- assess the thermal hydraulic analysis undertaken to support the PSA success criteria;
- assess the appropriateness and validity of the computer codes used in accordance with SAPs FA.17 to FA.24;
- commission TSCs to undertake independent confirmatory analysis of selected UK EPR transients;
- support the assessment of the internal and external hazards safety cases; and

- assess the safety case arguments and thermal hydraulic analysis of the containment response to design basis fault sequences which result in primary and secondary steam releases to the containment building.

18 The intention at GDA Step 3 was to review the thermal hydraulic analysis supporting the PSA success criteria during GDA Step 4. In practice an alternative strategy has been adopted in which the thermal hydraulic success criteria have been reviewed by a TSC (GRS, see Section 2.3.3 below) working for the PSA technical leads within ND. The work performed by GRS is reported in Ref. 17 and the PSA assessment is reported in Ref. 18. Hence, the PSA success criteria are not discussed further within this report.

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

20 Support has been provided to external and internal hazard topic leads in GDA Step 4 and is reported in Section 4. Finally, as noted in Section 2.3.1, the thermal hydraulic analysis supporting the design basis assessment of the containment response to fault conditions has been an area for assessment in GDA Step 4 but is reported in Ref. 16.

2.3.3 Use of Technical Support Contractors

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

22 Gesellschaft für Aglagen und Reaktorsicherheit (GRS) mbH undertook the majority of work in GDA Step 4 in the Fault Studies area. GRS has completed technical work in the following areas:

- development of a reactor physics model for UK EPR;
- development of a thermal hydraulic model for UK EPR;
- ATWT analysis using the developed reactor physics and thermal hydraulic models;
- assessment of heterogeneous boron dilution faults using Computational Fluid Dynamics (CFD) and the developed reactor physics and thermal hydraulic models; and
- cooldown fault analysis using the developed reactor physics and thermal hydraulic models.

23 The analyses undertaken with the models that were developed are discussed within the relevant faults areas in Section 4.2. The reactor physics and thermal hydraulic codes used by GRS are its own "in-house" codes and are independent of those used by EDF and AREVA. GRS utilised a commercially available code for the CFD analysis but again it is independent of the code used by EDF and AREVA for their equivalent assessment.

24 Information Systems Laboratories, Inc (ISL) has been used to undertake independent confirmatory analysis of LOCA faults within the design basis of the UK EPR. ND

provided ISL with a United States Nuclear Regulatory Commission (US NRC) model of the US EPR developed using the TRACE thermal hydraulic code. ISL adapted this for the specifics of the UK EPR (there are a number of differences between the EPR design proposed for the USA and that submitted for GDA in the UK) and then re-analysed the intermediate small break loss of coolant faults modelled by EDF and AREVA. The results of this work are discussed in Section 4.2.8.

25 The HSE SAPs (Ref. 4) set out numerical targets for the calculated radiological consequences for design basis fault sequences. In the PCSR (Ref. 12), EDF and AREVA have presented radiological consequences for identified fault sequences (for a generic site) but have not directly linked either the methodologies used or the resulting dose values with the UK expectations set out in Ref. 4. Serco was commissioned to review Chapter 14.6 of the PCSR (Ref. 12) and advise me on whether meaningful comparisons can be made between EDF and AREVA's radiological consequences and Target 4 in the HSE SAPs. Serco's conclusions are discussed in Section 4.3. It should be noted that site-specific calculations of radiological consequences are beyond the scope of GDA (see Section 2.3.6).

2.3.4 Cross-cutting Topics

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

- categorisation and classification of structures, systems and components (see Section 4.1.4);
- control and instrumentation (Section 4.1.2 and throughout Section 4.2);
- spent fuel pool faults (see Section 4.2.11);
- heterogeneous boron dilution faults (see Section 4.2.13);
- radiological source terms (see Section 4.3); and
- limits and conditions of safe operation (see Section 4.5).

2.3.5 Integration with other Assessment Topics

27 Specific key areas for co-ordinated work are:

- review of the EDF and AREVA assessment method for calculating radiological consequences following design basis fault sequences (in collaboration with radiation protection and chemistry topic leads);
- assessment of thermal hydraulic analysis undertaken to support PSA success criteria (in collaboration with the PSA topic lead);
- assessment of thermal hydraulic analysis undertaken to support structural analysis (in collaboration with the structural integrity topic lead);
- review of the design and sizing requirements of key safety components, e.g. heat exchangers, safety injection pumps, etc (in collaboration with mechanical engineering topic lead);

- assessment of the internal and external hazards safety case (in collaboration with the internal and external topic leads); and
- assessment of the spent fuel pool design, including the design of the racks, piping and cooling systems (in collaboration with many topic areas).

2.3.6 Out of Scope Items

28 The following items have been agreed with the RP as being outside the scope of GDA.

- Site specific calculations for radiological consequences – these will be provided as part of nuclear site licensing. EDF and AREVA have presented their methodology and some non-site specific generic results for the purposes of GDA.
- Control and limitation functions within the reactor control, surveillance and limitation (RCSL) system – these functions are used in normal operation of the plant and their detailed design is still being developed (they will in part be determined by the future UK EPR operator). Exceptions to this are those limitation functions that are used to protect against frequent fault transients that could result in fuel failures due to the PCI. However, these are discussed within the assessment of the fuel and core design under RO-UKEPR-42 and so are reported separately (Ref. 15).
- Operational Technical Specifications – the details of these are for a future operator to define as part of site licensing and have therefore not been assessed in GDA. Fault Studies have been involved in the definition of the Limits and Conditions as part of RO-UKEPR-55 (Ref. 10) which will feed into the future Technical Specifications. One specific aspect determined by Fault Studies that ultimately will need to be reflected in Technical Specifications are the uncertainty allowances to be included in the Departure from Nucleate Boiling Ratio (DNBR, see Section 4.2.5.3) setpoint calculations for the reactor protection system (RPS). While the statistical methodology proposed by EDF and AREVA has been examined during GDA Step 4, it has still to be applied to develop numerical limits on operation and therefore no uncertainty allowances have actually been assessed within GDA. Furthermore, EDF and AREVA have not provided any justification for the uncertainties associated with the calibration of the in-core detectors.
- Operation with mixed oxide fuel (MOX) in the reactor or the fuel handling facilities is outside the scope of GDA.
- As part of routine operations, the UK EPR will reduce the primary circuit inventory to "¾ loop" during shutdown. Faults from this state have been assessed as part of GDA. However, the PCSR (Ref. 12) does not present a sufficient safety case for steam generator maintenance activities with the fuel still loaded in the core. Future operators will have a choice of either undertaking such maintenance activities with the fuel removed from the reactor vessel or developing a safety case for undertaking maintenance activities at "¾ loop" with fuel still loaded. Assessment of such maintenance operations is therefore outside the scope of GDA.

3 EDF AND AREVA'S SAFETY CASE

29 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.

30 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 RPS 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.

31 The Fault Studies safety case in the PCSR (Ref. 12) is organised on a fault by fault basis. For each fault within the design basis, these engineered features and their associated supporting systems, are claimed to provide protection against the potential unmitigated consequences. The claims, arguments and evidence presented in the PCSR and supporting references has formed the basis of the assessment reported in next the section.

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

32 My assessment against the SAPs of the Fault Studies aspects of the UK EPR design basis analysis is presented below.

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

- Section 4.1.1 considers the fault categorisation system that has been applied by EDF and AREVA to the UK EPR.
- Sections 4.1.2 to 4.1.4 sections cover the approach to diversity and common mode failure, redundancy and the single failure criterion, and the implications of these on the categorisation and classification of structures, systems and components important to safety.
- Section 4.1.5 considers the general structure of EDF and AREVA's safety case.
- Section 4.1.6 looks at how EDF and AREVA have demonstrated that the list of initiating faults that they have identified is systematic, auditable and comprehensive.

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

35 Section 4.3 reviews the radiological consequences analysis of the bounding faults. Section 4.4 reviews how the limits and conditions identified from safety analysis will be captured in future updates to the safety case. Section 4.5 discusses how Fault Studies has provided support to the structural integrity assessment undertaken for GDA. Section 4.6 assesses the adequacy of Fault Schedule, which aims to summarise the totality of UK EPR design basis safety case. The final two sections discuss commissioning requirements resulting from the Fault Studies assessment and summarise the areas where HSE has co-operated with overseas regulators.

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

37 Some of the findings identified in Section 4 of this report are of particular significance and will require resolution before HSE ND would agree to the commencement of nuclear safety-related construction of a UK EPR reactor in the UK. These are identified in this report as GDA Issues.

4.1 General Aspects of the UK EPR Safety Case

4.1.1 Fault Categorisation

38 EDF and AREVA have classified all faults into four Plant Condition Categories (PCC) and two Risk Reduction Categories (RRC). 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.

39 The four PCC categories 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)

40 The first of the two risk reduction categories (RRC-A) 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)

41 RRC-A events typically represent multiple failure sequences in which there is a loss of a safety system claimed in the PCC analysis. These fault scenarios are traditionally treated as being within the design basis in the UK. To achieve the attributed core damage frequency, additional engineered features not considered in the PCC analysis are required. Without these features, the predicted sequence frequencies for core damage are within the range (>10^{-7} per year) for which design basis analyses are required (Ref. 19). RRC-A events are therefore assessed in this report with their associated PCC event.

42 Severe accidents are categorised as RRC-B faults. Discussion of severe accident sequences is deferred to Ref. 16.

43 EDF and AREVA aim to demonstrate that the effective dose to an individual off-site is less than the legal limit for normal operation and 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. An assessment of the methodology presented by EDF and AREVA, and discussion on the appropriateness of any comparisons to Target 4 is given Section 4.3.

4.1.2 Diversity and Common Mode Failure

44 SAP EDR.2 requires that appropriate use should be made of diversity within the designs of structures, systems and components (SSC) important to safety while SAP EDR.3 states that common mode failure should be explicitly addressed. In my GDA Step 3 Assessment Report, I noted that the fault categorisation scheme discussed above appears to be partially based upon the US ANSI / ANS 51.1 1983 standard (Ref. 20). 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. Chapter 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 (LOOP).

45 In the UK, it is considered good practice to regard any fault sequence with a frequency greater than 1 x 10^{-7} per year to be within the design basis (Ref. 19). 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, 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, RO-UKEPR-41 (Ref. 10) was 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. EDF and AREVA were requested to treat this analysis as an extension to the design basis analysis to be included within any future revision of the PCSR.

46 In their response to RO-UKEPR-41 (Ref. 45), EDF and AREVA have produced a matrix table in which each of the frequent PCC initiating faults are listed against each of the lower level safety functions of the reactor (see Section 4.1.4 below). This matrix is then used to identify the bounding frequent fault transient for each lower level safety function. For those transients not already covered by a PCC analysis, an additional fault transient has been studied in the response to RO-UKEPR-41. These additional analyses are reviewed together with the relevant PCC analysis on a case-by-case basis in the relevant fault specific discussion in Section 4.2 below. As a result of this work, EDF and AREVA have identified the need for some design changes to the Safety Actuation System (SAS)[1]. These changes are, again, discussed on a case-by-case basis in Section 4.2, and are captured as a GDA Issue on functional diversity, under **GI-UKEPR-FS-02**.

47 In line with HSE ND's expectation, EDF and AREVA have included the extended analysis produced for RO-UKEPR-41 within the March 2011 PCSR (Ref. 14), with the exception of those items still being developed through GDA Issue **GI-UKEPR-FS-02** (the GDA Issue is discussed further in Section 4.2). The outcomes of the GDA Issue should be captured within the subsequent revisions of the PCSR.

4.1.3 Redundancy and the Single Failure Criterion

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

49 In my GDA Step 3 Assessment Report, the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 were discussed with regard to passive single failure because of the definition of the design criterion used by EDF and AREVA. EDF and AREVA's design criteria only require passive failures to be considered within the single failure criterion after a period of 24 hours following an initiating event. In contrast, in the UK, passive failures are considered within the single failure criterion (Ref. 18). In addition, the failures of a non-return valve to open on demand and of a steamline isolation valve to close on demand are considered as active and not passive failures in the UK. For this reason, RO-UKEPR-41 (Ref. 10) also required 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.

[1] The SAS is independent of the RPS. It enables the processing of automatic and manual actions, together with the associated actions, including some F1B and F2 safety functions (see Section 4.1.4).

50 In their response to RO-UKEPR-41 (Ref. 21), EDF and AREVA have systematically reviewed all the frontline and support safety systems on the UK EPR (apart from the Heating, Ventilation and Air Conditioning (HVAC) system) with regard to passive single failures. The study demonstrates that the UK EPR is robust with regard to this design principle. The design is generally able to demonstrate tolerance to a passive single failure not only at the functional level as required by SAPs EDR.2 and EDR.4 but also at the more demanding system level.

51 RO-UKEPR-41 (Ref. 21) has identified the following areas where a passive single failure could potentially affect the performance of a safety function and for which it is required to demonstrate that the position is as low as is reasonably practicable (ALARP):

- a failure of pressuriser safety relief valve (PSV) to re-close on demand;
- a failure of the Main Steam Isolation Valve (MSIV) to close on demand;
- a break on the thermal barriers of the Reactor Coolant Pumps (RCP) cooling line
- a failure of a non-return valve on one for the safety injection lines of the safety injection system;
- a break on the steam generator blowdown transfer line following a steam generator tube rupture fault; and
- a break on the main steam isolating valve heater line.

52 The ALARP demonstration for the failure of PSV to re-close is discussed within the assessment of decrease of heat removal faults in Section 4.2.3 below while the ALARP demonstration for failure of an MSIV to close on demand is discussed in Section 4.2.2 below.

53 EDF and AREVA have still to perform a design basis assessment on the effects of a break on the thermal barriers of the RCPs cooling line. This will be provided as part of their response to GDA Issue **GI-UKEPR-FS-05** requiring a review of faults on the essential support systems, which is discussed further in Section 4.2.9 below.

54 The analysis of the passive single failure of the non-return valve on the safety injection system has been reported as part of the response to RO-UKEPR-57 (Ref. 22) on the modelling of PCC-4 LOCA faults and is discussed in Section 4.2.8.

55 EDF and AREVA's arguments on the acceptability of a break in the blowdown transfer line are assessed within the assessment of Steam Generator Tube Rupture (SGTR) faults in Section 4.2.8.2.

56 EDF and AREVA argue in Ref. 21 that the consequences of break on the main steam isolating valve heater line is bounded by the failure of an MSIV to close on demand and an SGTR fault with a stuck open Main Steam Relief Train (MSRT) valve. I accept this position. The acceptability of the safety case for the two bounding faults is discussed in Section 4.2.2.5.

57 There is one single passive failure that EDF and AREVA have not considered in their response to RO-UKEPR-41 (Ref. 21). This is the potential spurious actuation of the flooding valves in the containment spreading compartment which is discussed in the Containment and Severe Accident Assessment Report (Ref. 16).

4.1.4 Categorisation and Classification of Structures, Systems and Components

58 EDF and AREVA identify four types of safety functions in the PCSR (Ref. 12); F1A, F1B, F2 and non-categorised. An F1A safety function is a function that is required for a PCC event to reach the controlled state (defined as the core is subcritical, the heat removal is ensured in the short term, the core coolant inventory is stable and the activity releases remain tolerable). In my opinion, the controlled state should also include ensuring long-term control of reactivity (see Section 4.2.1.2). An F1B safety function is a function that is required to reach the safe shutdown state (defined as the core is subcritical, the decay heat is removed durably and the activity releases remain tolerable). F2 safety functions are claimed for RRC-A and RRC-B sequences.

59 A system is classified F1A, F1B, F2 or non-classified according to the classification of the highest integrity safety function it must perform. However, as there is generally a one to one relationship between the functions and the systems, the terminology F1A, F1B and F2 is used by EDF and AREVA for both functional categorisation and system classification. 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.

60 At the start of GDA Step 4, RO-UKEPR-43 (Ref. 10) on categorisation and classification was issued, which required EDF and AREVA to bring safety classification into line with the UK practice of using functional categorisation and SSC classification (as set out in SAPs ECS.1 and ECS.2). During GDA Step 4, in response to the requirements of RO-UKEPR-41 and RO-UKEPR-43, EDF and AREVA have been migrating over to an alternative categorisation and classification system, consistent with that used in the UK. This new system has been used in most of the responses to ROs in the Fault Studies area supplied during GDA Step 4, including the Fault Schedule.

61 EDF and AREVA's revised approach is set out their response to RO-UKEPR-43 (Ref. 23). In their responses, they identify the three main safety functions which are necessary for achieving the overall safety objective of protecting people and the environment from harmful effects of ionizing radiation:

- control of reactivity;
- heat removal; and
- confinement of radioactive material.

62 EDF and AREVA have further sub-divided these main safety functions into more detailed sub-functions called Plant Level Safety Functions (PLSF).

Main Safety Function	Plant Level Safety Function
Control of reactivity	R1 - Maintain core criticality control
	R2 - Shutdown and maintain core sub-criticality
	R3 - Prevention of uncontrolled positive reactivity insertion into the core
	R4 - Maintain sufficient subcriticality of fuel stored outside the RCS but within the site
Residual heat removal	H1 - Maintain sufficient RCS water inventory for core cooling
	H2 - Remove heat from the core to the reactor coolant
	H3 - Transfer heat from the reactor coolant to the ultimate heat sink
	H4 - Maintain heat removal from fuel stored outside the reactor coolant system but within the site
Radioactive material confinement	C1 - Maintain integrity of the fuel cladding
	C2 - Maintain integrity of the Reactor Coolant Pressure Boundary
	C3 - Limit the release of radioactive material from the reactor containment
	C4 - Limit the release of radioactive waste and airborne radioactive material
Other	O1 - Prevent the failure or limit the consequences of failure of a SSC whose failure would cause the impairment of a plant level safety function

63 The list of safety functions are further broken down into Lower Level Safety Functions (LLSF) which define how each PLSF are to be achieved through more detailed requirements. The full list of LLSFs is given in Ref. 23. A safety function category (A, B or C) is applied to each LLSF, using definitions consistent with SAP ECS.1.

64 The methodology then requires that the group of safety systems fulfilling each LLSF are identified. These groups of safety systems are known as a Safety Functional Group (SFG). The SFG is a group of SSCs that work together to perform an identified action contributing to the Safety Function. The safety classification is applied first at the SFG level; SFGs are classified on the basis of the most significant safety function that they perform. The SFG safety class is then applied to the SSCs.

65 The following safety class definitions are adopted:

- Class 1 – any SFG / safety feature that forms a principal means of fulfilling a Category A safety function;
- Class 2 – any SFG / safety feature that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function; and

- Class 3 – any SFG / safety feature that contributes to a category B function, or fulfils a category C function.

66 The final classifications of SSCs as a result of this process are summarised in Ref. 23 and are reflected in the Fault Schedule (Ref. 24). The practical effect of this new classification is that SSCs identified in the Fault Studies chapters of the November 2009 PCSR (Ref. 12) are effectively mapped over from F1A, F1B, and F2 to Class 1, Class 2, and Class 3 with the exception of those systems identified within the responses to RO-UKEPR-43 and RO-UKEPR-41 which provide functional diversity within the design basis. EDF and AREVA have been asked to upgrade these systems to Class 2 systems, subject to reasonably practicability. These actions will be completed under Action 5 of GDA Issue **GI-UKEPR-CC-01** (Ref. 25) for those frontline systems already identified under RO-UKEPR-43 or under Action 8 of GDA Issue **GI-UKEPR-FS-02** for those essential support systems that have yet to be reviewed.

67 While many of the RO responses (and this assessment report) principally utilise the revised approach to classification and categorisation, it has only been incorporated into the updated PCSR (Ref. 14) in a limited way. The chapters covering PCC and RRC-A events still continue to use the original EDF and AREVA categorisation and classification scheme.

4.1.5 Structure of the Safety Case

68 SAP FA.1 requires that fault analysis should be carried out comprising design basis analysis, probabilistic safety analysis and severe accident analysis. EDF and AREVA have approached this requirement by presenting the design basis accident analyses for the UK EPR in Chapter 14 of PCSR (Ref. 12) 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. These sources of information have been supplemented in GDA Step 4 by additional material that has been submitted in response to ROs 40, 41, 57, and 63. Overall, I judge that the extent of analysis largely meets the requirements of SAP FA.1 although in some limited areas, as discussed below, additional analysis will be required.

4.1.6 Fault Identification

69 SAP FA.2 requires that the process for identifying initiating faults should be systematic, auditable and comprehensive. In my GDA Step 3 Assessment Report, I noted that the UK EPR list of design basis faults did not appear to include support system faults and control and protection faults. It was not clear therefore that the list of faults was comprehensive. In contrast, the list of initiating events for the PSA presented in Chapter 15 of the PCSR was based upon a systematic failure modes effects analysis of the UK EPR systems. Recognising that, in principle, any initiating event identified in the PSA should be included within (or bounded by) a design basis initiating event unless it is screened out on the basis of low frequency (as is acknowledged by SAP FA.5), I raised RO-UKEPR-40 requesting EDF and AREVA to reconcile the list of design basis initiating events with the list of PSA initiating events with the aim of demonstrating that the list of

design basis initiating events considered within the PCSR was as comprehensive as possible.

70 In their response to RO-UKEPR-40 (Ref. 26), EDF and AREVA have very clearly and systematically reviewed the list of PCC design basis initiating events against the list of PSA initiating events. The response reviews primary system breaks, transient events in the primary system, including heterogeneous boron dilution events, support system failures, including loss of cooling chain events, secondary system breaks, SGTR failures, transient events in the secondary system, LOOP events, anticipated transients without trip events, shutdown faults, and fuel pool faults. The scope of EDF and AREVA's review is comprehensive apart from the coverage of those systems whose design is not yet sufficiently well developed (the HVAC system, the electrical system, the C&I systems and some of the cooling chain systems) to have been included within the PSA. In addition, internal and external hazard initiating events are not considered.

71 The conclusion of the review is that the existing coverage of design basis faults is generally comprehensive. However they have identified that the following initiating events are not considered within the design basis list of PCC initiating events: loss of cooling chain faults, spurious C&I faults, internal and external hazards, HVAC faults, heterogeneous boron dilution faults and induced (or consequential) SGTR faults. All these faults are discussed on a case-by-case basis in Section 4.2 below.

72 Of these faults, EDF and AREVA have acknowledged there is a need for some design basis analysis to be performed on the design of the support systems comprising the cooling chain to the ultimate heat sink, and possibly the designs for the HVAC and electrical systems. Since these reviews can potentially result in design changes to these systems, completion of these items has been raised as GDA Issue under **GI-UKEPR-FS-05**. As noted in Section 2.3.6, the control and limitation functions from the RCSL system are out of the scope of GDA. However, once detail design is complete, this system will also need to be reviewed for potential fault initiators.

73 As discussed in Section 4.2.13 below, a separate GDA Issue, **GI-UKEPR-FS-01**, has been raised to cover heterogeneous boron dilution faults.

74 Consequential SGTR faults are discussed in Section 4.2.2 below but EDF and AREVA have performed additional analysis and claim that they are adequately bounded by existing PCC events.

75 Internal and external hazards are also discussed below. EDF and AREVA have traditionally handled such events separately from the PCC analysis. This approach may be acceptable, but it is important to ensure good visibility of the safety case and the categorisation and classification of the safety barriers that protect against these events. Hence, under Action 3 of cross-cutting GDA Issue, **GI-UKEPR-CC-01**, EDF and AREVA will be asked to include these items within the Fault Schedule or some other suitable format agreed with HSE ND (Ref. 25).

4.2 Fault Sequences

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

and risk reduction sequence analysis performed by EDF and AREVA will be reviewed in turn for each of the following fault categories:

- reactor trip faults;
- increase in heat removal from the primary system;
- decrease in heat removal by the secondary system;
- electrical supply faults;
- decrease in reactor coolant system flow rate;
- reactivity and power distribution anomalies;
- increase in reactor coolant inventory;
- decrease in reactor coolant inventory;
    i) SGTR;
    ii) Small Break LOCA (SBLOCA);
    iii) Intermediate and Large Break LOCA (IBLOCA and LBLOCA) within the design basis;
    iv) double-ended guillotine break of primary coolant main pipework (2A-LBLOCA);
- other (support) system faults;
- control and protection faults:
- spent fuel faults;
- shutdown faults;
- heterogeneous boron dilution faults;
- internal hazards; and
- external hazards.

4.2.1 Reactor Trip Faults

4.2.1.1 Summary of EDF and AREVA's Safety Case

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

78 The basis of the EDF and AREVA safety case is that a spurious reactor trip is a less severe transient than any other PCC-2 transient and so can be bounded by the loss of condenser vacuum fault which results in a turbine trip and a consequential reactor trip. This fault is included in the list of a decrease in heat removal faults, which are discussed further in Section 4.2.3 below.

4.2.1.2 Assessment

79 While it is accepted that from a transient analysis perspective this fault can be bounded by other more onerous transients, I have concerns about the long term control of reactivity aspects of this fault given its high initiating frequency. This is because following every reactor trip there will be an eventual reduction in the shutdown margin of the reactor core due to the decay of xenon. While the Extra Boration System (EBS) and the IRWST systems provide diverse sources of borated water should the operator fail to ensure adequate shutdown margin using the Chemical and Volume Control System (CVCS), both these systems are also dependent upon operator action for actuation. Although the timescales are long (many hours) this implies a combined human reliability claim on the operator action of 1×10^{-7} per demand to meet the design basis target. In the case of Sizewell B, there is an automatic actuation of the CVCS following every reactor trip to protect against this possibility. For this reason, Action 6 has been raised as part of the GDA Issue on diversity, under **GI-UKEPR-FS-02**, requesting EDF and AREVA to consider the feasibility automatically actuating the CVCS system to inject borated water after every reactor trip and for the EBS to be automatically actuated following the failure of the CVCS (or alternatively to provide a consequence argument should the operator fail to ensure an adequate shutdown margin).

4.2.1.3 Findings

80 Under Action 6 of the GDA Issue on diversity, **GI-UKEPR-FS-02**, EDF and AREVA are required to review the issue of diversity for long term reactivity control. They are to consider the feasibility of automating the operation of the EBS following every reactor trip or to provide a consequence argument should the operator fail to ensure an adequate shutdown margin.

4.2.2 Increase in Heat Removal Faults

4.2.2.1 Summary of EDF and AREVA's Safety Case

81 Faults in this category result in a cooldown of the primary circuit. Given the negative moderator temperature coefficient of a Pressurised Water Reactor (PWR) such faults result in an increase in the reactivity and power of the core potentially threatening the integrity of the fuel cladding should a departure from nucleate boiling (DNB) occur. If a reactor is initially in the hot zero power condition, it may return to power as a result of the positive reactivity feedback induced by the cooldown, 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. 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.

82 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 fault. For those cases which they consider to be limiting, they have performed detailed analyses. EDF and AREVA claim that these demonstrate, even for the most bounding faults, the RPS is able to trip the reactor and

isolate the affected steam generator to reduce the rate of reactor cooldown, ensuring an adequate shutdown margin.

83 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 MSIV and a stuck open valve on either the MSRT system or 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 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 RCCA with the most worth 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.

4.2.2.2 Assessment (Overview)

84 EDF and AREVA have identified 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; and
- steam system piping failure.

85 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.

86 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.

87 In the sections below, I have separately presented my assessment of the limiting steam system piping failure (Section 4.2.2.3) from my assessment of the two bounding frequent faults (Section 4.2.2.4). I have also commented on EDF and AREVA's safety case on consequential failures, achieving safe shutdown and the assessed radiological consequences from increase in heat removal faults (Sections 4.2.2.5 to 4.2.2.7). Section 4.2.2.8 summarises my assessment of the MANTA computer code.

88 Note that an assessment of the thermal hydraulic response of the containment building to these faults has also been made but this is reported separately (Ref. 16).

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

Fault Sequence Analysis

89 The analysis of the steam system piping failure 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 x 10^{-4} and 1 x 10^{-6} per year. For Sizewell B (Ref. 27) a main steam line rupture inside containment was assumed at 1 x 10^{-4} per year while one outside containment was conceded at 1 x 10^{-3} per year. Such frequencies would be consistent with the assumption of a PCC-3 or PCC-4 event. While such event frequencies can be considered infrequent, they are within the design basis according to SAP FA.5 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.

90 EDF and AREVA have treated the fault as being within the design basis meeting the requirements of SAPs FA.4 and FA.5. The single failure they choose to consider is failure of the RCCA with the most worth to enter the core following reactor trip. The assumption of a stuck out RCCA is one of the standard deterministic assumptions made within the transient analysis studies of cooldown faults such as those considered here. It is a major factor in determining the shutdown margin of the reactor and whether the core returns to criticality following reactor trip. Making this assumption helps ensure that the overall assessment is conservative, consistent with the requirements of design basis analysis. It is not normal practice in the UK (Ref. 27) to consider this assumption to count as the single failure for the fault. Instead, an additional single failure is normally included within the analysis. However, in practice this is not considered to be a problem with the EDF and AREVA analysis, given that the feedwater lines are provided with redundant isolation valves and the steam line break on the affected Steam Generator (SG) is not assumed to be isolated (so bounding any single failure of a MSIV). Given that the protection signals that are claimed are all based upon 2-out-of-4 voting logic, the next most onerous failure is probably a failure of one of the Medium Head Safety Injection (MHSI) pumps to operate on demand. In their analysis for the PCSR (Ref. 12), EDF and AREVA do not model this single failure but instead 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)[2]. Hence, I judge that the requirements of SAPs FA.6, EDR.2 and EDR.4 are met.

Methods and Assumptions

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

- A bounding shutdown margin is used which assumes that the highest worth RCCA remains stuck out of the reactor following reactor trip. The calculation of shutdown margin is detailed in Chapter 4 of the PCSR (Ref. 12) and includes a number of allowances for calculational uncertainty. The calculation assumes hot zero power conditions at end of cycle (EOC) but with equilibrium xenon conditions.
- A maximum moderator density coefficient is chosen. The value varies slightly depending on the particular cases studied but it is typically about -95 pcm/°C. This is an EOC value for which the boron concentration in the core is close to zero

[2] In some later analysis undertaken for RO-UKEPR-63 (Ref. 43) the MHSI water is assumed to be borated. However the conclusion reached here on the adequacy of the safety case presented in the PCSR (Ref. 12) is unaffected.

making the moderator coefficient most negative, which is conservative for cooldown transients.

- The differential boron coefficient is minimised to reduce the effectiveness of any borated water injected in from safeguard systems such as the MHSI and EBS.
- A minimum Doppler temperature coefficient is used to maximise the peak return to power. The delayed neutron fraction is also minimised to increase the rate of return to power.
- No residual heat is modelled to maximise the cooldown rate prior to return to criticality. A maximum value is assumed for the heat transfer coefficient from the fuel pellet to the clad. This minimises the Doppler effect in the fuel and so maximises the return to power. It also maximises the transfer of heat to the clad so maximising the potential for DNB.
- The flow from the main feedwater and emergency feedwater systems is generally maximised in a bounding way to enhance the rate of cooldown from the steam generators. In addition, the RPS setpoints for actuating reactor trip and for safeguard actuation and the delay times on safety guard actuation signals include conservative allowances for errors and uncertainties.
- The modelling of steam flow through the break assumes perfect moisture separation within the steam generator resulting in a discharge quality of 1.0, which maximises the cooling efficiency of the steam generator as it depressurises.

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

93 EDF and AREVA have utilised a complex calculational route (Refs 28 and 29) to analyse these faults, which couples together three computer codes called MANTA, SMART and FLICA III. MANTA is a thermal hydraulic code (Refs 30 to 33) used to model the primary system cooldown transient. SMART is 3D reactor kinetics code and is part of the larger SCIENCE reactor physics code (Ref. 34). SMART models the neutronic response of the core. FLICA III is a thermal hydraulic sub-channel code (Refs 35 to 37) used to determine whether the fuel in a localised area of the peak fuel assembly enters into DNB. EDF and AREVA have coupled these codes together to provide a code package that is capable of modelling most intact circuit faults on a PWR including steamline breaks, rod ejection faults and anticipated transients without trip (where a frequent initiating event occurs and the reactor fails to trip). The MANTA code can also be used separately, together with its own point kinetics model, for a range of simpler faults where the reactor rapidly trips such as the loss of normal feedwater fault.

94 Given the importance of this calculational route, I decided in my GDA Step 3 Assessment Report (Ref. 6) that there was a need to sample the validation of the MANTA, SMART and FLICA III computer codes. For this reason, the validation evidence for all three codes has been assessed during GDA Step 4 against a relevant selection of the assurance of validity SAPs FA.17 to FA.24. In the case of the FLICA III and SMART, the assessment of their validation is reported in the Fuel and Core Assessment Report (Ref. 15). The validation of the MANTA code is reported here, in Section 4.2.2.8 below.

In summary, all these assessments conclude that the methods deployed by EDF and AREVA for the analysis of these faults are fit for purpose, although a number of Assessment Findings are identified to help improve the validation evidence for the codes.

Transient Analysis

95 SAP FA.7 also requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. EDF and AREVA's safety criteria for PCC-3 and 4 events is that less than 10% of the fuel rods undergo DNB. In practice, for faults considered in this section, the aim of EDF and AREVA is to demonstrate this is achieved by ensuring the fuel cladding maintains efficient heat transfer to the water and does not undergo DNB. In my opinion the latter objective represents relevant good practice in the UK and the ALARP position. To confirm that this objective has been achieved, the results of design basis analysis of EDF and AREVA need to be assessed.

96 I have assessed the results of the base case analysis presented within the PCSR and have compared them with similar analysis for Sizewell B. I have also considered additional sensitivity studies performed by EDF and AREVA in response to RO-UKEPR-63 looking at:

- the effectiveness of the MHSI system;
- the effectiveness of the EBS;
- the effect of the tripping the RCPs;
- the assumptions on equilibrium xenon conditions; and
- the effect of break size and power level.

97 Finally, I have compared the results of a revised base case with independent analysis of the same fault performed by one of our TSCs (Ref. 38).

98 Much of the analysis presented in the PCSR for the steam line break upstream of the MSIV was not specifically performed for the UK EPR design. Instead, the PCSR presents an analysis undertaken for a 4250 MWth reactor design, together with a sensitivity study for a 4500 MWth reactor design. The results of the EDF and AREVA analyses are summarised in Fig. 5 of Chapter 14.5.2 of the PCSR for the 4250 MWth reactor and in Fig. 41 for the 4500 MWth reactor. These figures present the return to power transients for these cases as a function of time. For the 4250 MWth case, the power peaks at 355 seconds at 17.3% while, for the 4500 MWth case, the power peaks at 405 seconds at 15%. These values are consistent given that the shutdown margins quoted in Table 1 and Table 8 of Chapter 14.5.2 of the PCSR are -2700 pcm and -3400 pcm respectively for the 4250 MWth and 4500 MWth EPR reactors. The cooldown transient results in the vessel inlet temperature reducing by about 100°C, which is sufficient to overcome these shutdown margins and return the reactor to power. The flux peaking factors associated with the worst RCCA being stuck out are not given. These cases assume that the RCPs do not trip. Once the affected SG 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 SG. The operator is assumed to isolate the EFWS to the affected SG after 30 minutes and commence boron injection using the EBS. This causes the reactor to shutdown.

99 To demonstrate that there is a margin to DNB, EDF and AREVA calculate the maximum heat flux for the most limiting fuel assembly and compare the value with the critical heat flux (CHF) for those conditions at which DNB is predicted to occur, generating a DNB ratio (DNBR). EDF and AREVA calculate the minimum DNBR to be 1.42 at 255 seconds for the 4250 MWth reactor and 2.12 at 425 seconds for the 4500 MWth reactor using their own "FC" CHF correlation (Ref. 12). This meets the requirements of the design basis DNBR limit of 1.12 which they adopt for the low pressure conditions that are associated with cooldown faults. In my GDA Step 3 Assessment Report (Ref. 6), I noted that these values are low when compared with the design basis value of 2.0 that it is applied at Sizewell B which uses the "Groeneveld" correlation for assessing CHF at low pressure (Ref. 39). The value of 2.0 was chosen to give sufficient margin to cover the statistical uncertainties that apply to the CHF correlations for low pressure, high quality conditions, although it should be noted that the experimental test data underpinning the Groeneveld correlation are now dated. For this reason, the recent experimental tests performed to develop the FC critical heat flux correlations used by EDF and AREVA have been reviewed in GDA Step 4 (Ref. 40 and TQ-EPR-242, TQ-EPR-681 & TQ-EPR-1302 as per Ref. 9). The assessment of this work is reported in the GDA Step 4 Assessment of the fuel and core design (Ref. 15) and it concludes that a convincing case has been made to support the CHF assessment method used for the analysis of fuel safety margins in normal operation and faults. In addition, I note from my own review of the test results provided in response to TQ-EPR-1302 (Ref. 9), that there is good data coverage in the low pressure, high quality region provided by the test results confirming that the low uncertainty allowances which EDF and AREVA are assuming for these faults are appropriate.

100 The 15% peak return to power reported in the EDF and AREVA analyses presented in the PCSR for the 4500 MWth reactor can be compared with the Sizewell B analyses (Ref. 27) which predicts a 14% peak return to power and a minimum DNBR of 2.27. The higher peak return to power is slightly surprising since the UK EPR possesses a much larger shutdown margin than Sizewell B (although the UK EPR reactor core is larger than the Sizewell B reactor core, it contains proportionally more shutdown RCCAs). For Sizewell B, the minimum end of life shutdown margin with the worst RCCA stuck in its fully withdrawn position is -1300 pcm (Ref. 27) compared with the minimum shutdown margins of -2700 pcm and -3400 pcm quoted above for the EPR reactors. One reason for the higher return to power is that EDF and AREVA are assuming of moderator temperature coefficient of -95 pcm/°C. This is thought to be more onerous than the moderator temperature coefficient assumed in the Sizewell B analysis (Ref. 27). In my GDA Step 3 Assessment Report, I speculated that another reason could be due to the modelling assumptions for the safety injection systems. For this reason, RO-UKEPR-63 (Ref. 10) requested EDF and AREVA to perform a sensitivity study modelling the MHSI in a more realistic way assuming only the loss of a single train to take account of the single failure criterion. This is discussed below.

Sensitivity to Medium Head Safety Injection Performance

101 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. The assumption of unborated water is somewhat arbitrary and does not give a realistic appreciation of the capability of the MHSI, which is qualified to safety system standards, for protecting against this fault.

102 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.

103 In an initial response to RO-UKEPR-63 (Ref. 41), EDF and AREVA presented analysis for a revised reference case and compared it with analysis for a sensitivity case in which the MHSI is modelled realistically apart from assuming the failure of a single train. In the revised reference case, the mixing assumptions in the lower plenum of the reactor vessel have been changed from those previously assumed. In determining the inlet temperature conditions for the MANTA calculation, the new analysis assumes that 73% of the total flow (entering from the affected quadrant) is mixed with the remaining 27% of the flow from the three unaffected loops before entering the core quadrant associated with the affected steam generator. This contrasts with original case presented in the PCSR (Ref. 12) in which it is assumed that 86% of the flow is mixed with the other quadrants. This change in the assumptions affects the rate of cooldown of the affected quadrant and results in the peak return to power reducing from 17.3% to 12.9% (comparing cases with the same shutdown margin). This change in the mixing assumptions is discussed further as part of the validation assessment of the MANTA code in Section 4.2.2.8 below, where it is concluded that the change is justified.

104 In the sensitivity case (Ref. 41), the MHSI is modelled more realistically by assuming the injection of water with a boron concentration of 2305 ppm. However, the peak power hardly changes going from 12.9% to 12.2%. The reason the MHSI has so little effect on the transient is that it is not functionally capable of injecting sufficient borated water into the core by the time of the peak return to power. The transient suggests that the medium head pumps on the UK EPR are largely ineffective in providing protection against cooldown faults compared with the high head pumps provided on Sizewell B. However, this effect is largely off-set by the larger shutdown margins available on the UK EPR. This is a legitimate design decision that has been made by EDF and AREVA recognising that the reason for choosing a MHSI system on the UK EPR was to provide better protection against the SGTR faults as discussed in Section 4.2.8 below. Indeed, it could be argued that increasing the shutdown margin is a more passive means of achieving this safety function rather than relying on active systems to inject extra borated water in keeping with the thinking behind SAP EKP.5.

Sensitivity to Extra Boration System Performance

105 Given the reduced effectiveness of the MHSI for such faults, EDF and AREVA were requested to consider the feasibility of automating the injection of borated water from the EBS. On the current UK EPR design there is a claim on operator action after 30 minutes to initiate EBS injection. Such a claim does not meet the requirements of SAP ESS.8, which requires that all safety systems should be automatically initiated. In response, EDF and AREVA informed HSE ND that they were already developing proposals to automate the actuation of the EBS system on low SG pressure under design modification Change Management Form (CMF) CMF#25 (Ref. 42).

106 In a second response to RO-UKEPR-63 (Ref. 43), EDF and AREVA have performed an additional sensitivity study to understand the effectiveness of this modification. For this analysis, EDF and AREVA revised their reference base case again, increasing the assumed shutdown margin from -2700 pcm to -4000 pcm to more accurately reflect the UK EPR core design. As a result of this change, the peak return to power has reduced from 12.2% to 4.4%.

107 For the EBS sensitivity study, EDF and AREVA have not considered a single failure on one of the two EBS trains, but this is not considered significant given the results of the analysis. The early introduction of EBS flow is seen to only slightly reduce the peak return to power from 4.4% to 3.8%. A study of the boron concentration plot shows that the boron concentration at the core inlet is only about 20 ppm by the time of peak return to power. This will only contribute about 100 pcm of negative reactivity.

108 It should be recognised that for slightly less bounding transients or more realistic modelling assumptions, the return to power will be slower providing more time for the EBS to inject and be effective providing the SG pressure falls sufficiently quickly to initiate the EBS on low SG pressure. In contrast, the MHSI system will be less effective for slower transients because the primary circuit pressure is unlikely to fall below the head pressure of the pumps. However, the main advantage of automatically initiating the EBS flow is that it ensures that the reactor returns to shutdown conditions more quickly. For these reasons, the introduction of modification CMF#25 (Ref. 42) to automate the actuation of the EBS injection on low SG pressure is supported since it increases the effectiveness and reliability of the EBS in such faults.

Sensitivity Study to Reactor Coolant Pump trip

109 The analysis reported in the PCSR (Ref. 12) assumes that the RCPs do not trip. This is because EDF and AREVA argue that this assumption maximises the cooldown rate of the primary system and so maximises the peak return to power. It is possible that a reactor and turbine trip will result in a loss of the grid. Indeed, EDF and AREVA's design basis methodology requires them to consider the consequential LOOP following turbine trip within their design basis sequences should this make the transient more onerous. In this case though, they consider it will not make the transient worse and the RCPs are assumed to continue to operate. However, in the case of a steamline break occurring within containment, there is a second reason why the RCPs might trip. The RPS isolates the containment building upon receipt of a high containment pressure signal. This causes the CCWS to be isolated. In order to protect the RCPs against loss of CCWS to their seals, the RPS trips the RCPs at the same time that it isolates the CCWS. Therefore, even if there is not a loss of off-site power, the RCPs could be tripped on high containment pressure at any point within the transient depending upon the size and location of a break.

110 For this reason, RO-UKEPR-63 (Ref. 10) requested EDF and AREVA to perform a sensitivity study in which the RCPs are tripped at the peak return to power to explore what effect this has upon the predicted minimum DNBR due to natural circulation conditions. EDF and AREVA performed three calculations, tripping the RCPs at the time of peak increase in core reactivity, at peak power, and at minimum DNBR. In all cases, the analysis suggests that the reduction in flow causes a decrease in the cooldown rate of the core and a reduction in the density of the moderator with a consequential reduction in reactor power level. This more than outweighs the effect of the reduction in flow on the minimum DNBR and therefore confirms EDF and AREVA's claim that assuming the RCPs continue to operate is bounding. However, the validation evidence for the mixing coefficients assumed in the lower plenum for natural circulation conditions has yet to be provided to HSE ND by EDF and AREVA for assessment. For this reason, an Assessment Finding, **AF-UKEPR-FS-01**, has been raised, requiring future operators to provide this information. In addition, I have concerns about the applicability of the critical heat flux correlation used in the analysis of main steamline break faults for natural circulation conditions following the tripping of the reactor coolant pumps. For this

reason, I have raised Assessment Finding **AF-UKEPR-FS-02** for a future licensee to justify the correlation applied.

111 It is understood that EDF and AREVA are intending to introduce a design change to automate the tripping of the RCPs in response to such faults. The studies reported above suggest that this represents a potential safety improvement on the UK EPR design that HSE ND should support subject to the validation evidence for the mixing coefficients being satisfactory, as discussed above and in Section 4.2.2.8.

Sensitivity to Xenon Level

112 The Case 1 transient reported in the PCSR (Ref. 12) assumes equilibrium xenon conditions at the time of the fault with the reactor at hot zero power. It is accepted that the choice of hot zero power is bounding for the double-ended guillotine break of a main steamline in terms of the resultant peak return to power following reactor trip. However, the choice of hot zero power is made to cover the full reactor operating power range from 0% to 100% power and so, in principle, the xenon level can be at any intermediate range, potentially changing the shutdown margin available by about 3000 pcm. It was therefore initially unclear if the assumption of equilibrium xenon conditions was a bounding one.

113 For this reason, RO-UKEPR-63 (Ref. 10) requested EDF and AREVA to perform a sensitivity study to initial xenon concentration. The sensitivity study predicts a higher return to power of 6.1% but the predicted minimum DNBR is higher at 4.02. EDF and AREVA have stated that this is due to higher peaking factors in the xenon free case. This is slightly surprising given that the effect of xenon poisoning is generally to reduce flux peaking in the higher power regions of the core. The reason is that EDF and AREVA have considered an extreme power distribution due to a load following transient that has resulted in a temporarily top peaked axial profile.

114 In practice, it must be recognised that the operator would increase the boron concentration to maintain adequate shutdown margin and this would have the benefit of making the moderator temperature coefficient more positive from that assumed in the reference case, which assumes zero boron concentration.

115 It is judged unreasonable to request EDF and AREVA to consider as a credible design basis fault sequence a cooldown fault occurring on a reactor at hot standby conditions with zero xenon and boron concentrations and a RCCA stuck out of the core. Without the presence of a stuck RCCA, the reduced flux peaking factors would probably ensure that there is an adequate margin to DNB. As an Assessment Finding, **AF-UKEPR-FS-03**, a future licensee is required to review the case of steamline break occurring at hot zero power conditions with zero xenon and boron concentrations but with all RCCAs inserted. It is noted that the Case 4 transient reported in the PCSR (Ref. 12) for a spurious MSRT opening is a similar transient to the steam line break case requiring review through the Assessment Finding. This case demonstrates significant margin to DNB.

Sensitivity to Break Size and Power Level

116 In my GDA Step 3 Assessment Report (Ref. 6), I noted that no sensitivity studies to break size and power level were presented within the PCSR (Ref. 12). I contrasted this with a report produced for Sizewell B (Ref. 27) which 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 judged that the Sizewell B results would give an indication of the sensitivity to these parameters for the UK EPR.

The Sizewell B report demonstrates that it is bounding for the larger breach sizes to start the transient calculation from the hot zero power condition in terms of the minimum DNBR, assuming the reactor trips 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. I noted that these results appeared to contradict the EDF and AREVA analyses, which assumed that starting at zero power was bounding for both the main steam line break fault and the stuck open / spuriously opened valve on the MSRT or MSSV systems. For this reason, RO-UKEPR-63 (Ref. 10) requested EDF and AREVA to produce further sensitivity studies to break size and power level to confirm the conclusions of their analysis during GDA Step 4.

117 In their response to RO-UKEPR-63 (Ref. 43), EDF and AREVA present two sets of sensitivity studies, one at hot zero power and one at full power, in which the assumed break size is varied as the sensitivity parameter. Not surprisingly, for the hot zero power case the minimum DNBR falls with increasing break size until the steam flow restrictor starts to limit the steam flow from the SG (after which the predicted DNBR value remains constant up to the limiting double ended guillotine break size). The minimum DNBR value for hot zero power case never falls below 3.0. For intermediate breaks from full power, minimum DNBR values below 1.0 are predicted. In contrast, for larger break sizes up to the double ended guillotine break, the minimum DNBR values are essentially unchanged from the pre-fault normal operating value. This is because for large break sizes the high SG pressure drop trip signal is very effective, tripping the reactor quickly and so limiting the reduction in the minimum DNBR value. For intermediate break sizes, the increase in the secondary steam flow is insufficient for this trip parameter to be effective. Reliance therefore has to be placed upon flux protection or SG water level which delays the time to reactor trip.

118 A study of those transients where the minimum DNBR is less than 1.0 (i.e. intermediate breaks sizes) demonstrates that DNB is only experienced for a very short period of time (31 seconds in the worst case) and affects only a limited amount of fuel (less than 2%), which EDF and AREVA claim meets their 10% criteria for PCC-4 fault conditions. In my judgement, this position is not ALARP since it should be possible to tighten or improve the protection to trip faster so as to prevent DNB. A related concern is the adequacy of protection for the frequent excessive increase in secondary steam flow discussed below. For this reason, Action 2 has been raised under **GI-UKEPR-FS-02** requesting EDF and AREVA to improve the protection against this fault. For more frequent smaller break sizes corresponding to the opening of the MSRT or an MSSV, EDF and AREVA claim that DNB is not predicted to occur. However, for the case of an MSRT valve spuriously opening, the minimum DNBR value falls to 1.16. This is below the safety limit of 1.21 that applies when the reactor pressure is greater than 120 bar. This may be acceptable because EDF and AREVA envisage that an additional uncertainty factor will be applied to the initial pre-fault limiting DNBR value during operational demonstration of compliance with the site technical specifications. However EDF and AREVA have not provided the methodology for determining the uncertainty allowance associated with the in-core detectors within GDA Step 4 and so this will need to be assessed for adequacy as part of site licensing. I have raised Assessment Finding, **AF-UKEPR-FS-04**, requiring a licensee to provide this methodology during site licensing.

Confirmatory Analysis

119 GRS has repeated the steamline break analysis from hot zero power using its own ATHLET systems code and its own 3D QUABOX/CUBBOX reactor kinetics code coupled together. The results of the GRS comparison (Ref. 38) show good agreement with EDF and AREVA predictions on the secondary side. As noted above, the EDF and AREVA modelling of steam flow through the break assumes perfect moisture separation within the SG resulting in a discharge quality of 1.0. GRS assume a homogeneous equilibrium model to represent the flow through the flow limiter. This results in the entrainment of water through the break. Entrainment is to be expected given that water will be flashed off in the affected SG as it depressurises. This means that the results of the GRS analysis will be more realistic than the conservative AREVA results. The GRS modelling predicts that the affected SG will dry out after 200 seconds. From this point the GRS transients diverge from the EDF and AREVA's transients as the cooldown finishes and the cold leg temperatures start to increase. Nevertheless, the results before 200 seconds show good agreement. The primary pressures are similar although the EDF and AREVA analysis predicts a slightly greater cooldown as would be expected given the differences in the break flow modelling.

120 The agreement of the transients in terms of changes in reactivity and power levels is less good. In my opinion, this is because the GRS model does not have the ability to model a neutron source on a shutdown reactor at zero power. To overcome this shortfall GRS has run a null transient to obtain the hot zero power steady state that is assumed in the EDF and AREVA analysis. In performing the null transient, GRS appear to have set the initial neutron population to very low value and so there is a significant delay during the transient while the neutron population grows. This appears to result in a large peak in reactivity. In contrast, the EDF and AREVA calculation predicts a quicker return to power but the peak in reactivity is smaller. Nevertheless, the integrated area under power transient curves looks broadly comparable as does the power removed by the secondary side up to the first 200 seconds. Despite the possible limitations in the GRS analysis, I consider that the GRS results are supportive of the EDF and AREVA analysis.

4.2.2.4 Assessment of Excessive Increase in Secondary Steam Flow (Limiting Frequent Fault)

Fault Sequence Analysis

121 EDF and AREVA have identified that a stuck open steam relief or safety valve following a normal operational transient is a PCC-2 event while a spurious operation of these valves is a PCC-3 event. They also recognised that an excessive increase in secondary steam flow fault is a PCC-2 event. As these initiating faults essentially result in a similar plant transient prior to reactor trip, they are considered together as a single bounding fault in the remainder of this section. Given that a PCC-3 can be as frequent as 1×10^{-2} per year, such events must be considered to be frequent events and so EDF and AREVA have reviewed these faults in their response to RO-UKEPR-41 (Ref. 10) in order to demonstrate functional diversity.

122 In their response to RO-UKEPR-41 (Refs 45 to 46), EDF and AREVA have identified the need to study two ATWT events following an excessive increase in secondary steam flow event. The first case is due to a common mode failure resulting in the mechanical failure of the RCCAs to insert. The second case is due to a common mode failure of the RPS to detect the fault and trip the reactor.

Transient Analysis

123 The case of excessive increase in steam flow with failure of RCCAs to insert is seen to cause a corresponding increase in reactor power from 100% to 115%. The minimum DNBR is claimed to remain above 1.0 although no plot is presented. In a later TQ response (TQ-EPR-1432, Ref. 9) EDF and AREVA claim to show that the DNBR remains greater than 1.9 when calculated using the MANTA, SMART, and FLICA III coupled codes but the timings on the transient look inconsistent to those of the earlier transient. In the initial analysis provided in response to the RO (Ref. 46) beginning of cycle (BOC) conditions with a moderator coefficient of -34 pcm/°C and an initial boron concentration of 1594 ppm are assumed, which are claimed to be bounding on the grounds they minimise the power reduction once the RCPs are tripped. Given that the initiating event is a cooldown transient, my concern is more with the initial reduction in the minimum DNBR and so it is not obvious that these assumptions are bounding. Furthermore, the minimum DNBR occurs before the time when normal reactor trip would occur anyway and so this is an issue associated with the effectiveness of 1st line tripping and not the low frequency ATWT sequence. The reactor trip signal occurs on low SG level after 313 seconds and turbine trip follows shortly afterwards causing reactor power to decrease. The ATWT signal occurs at 333 seconds following failure of the RCCAs to insert, causing the EBS to inject borated water. The RCPs are tripped after 397 seconds on low SG level.

124 As with the stuck RCCA ATWT case, the excessive increase in steam flow with failure of the protection system case causes the reactor power to increase from 100% to 115% and the minimum DNBR decreases to a value of 1.1. The analysis again assumes BOC conditions. However, the failure of the RPS means that the reactor can only be tripped on the diverse protection system which results in a significant delay in the trip which does not occur until 923 seconds.

125 These same faults are also studied in the RRC-A analysis in Chapter 16.1 of the PCSR (Ref. 12). It is noticeable that the transient studies performed in the response to RO-UKEPR-41 are significantly more penalising than the ones reported in the RRC-A. These differences are judged to be more than can be explained by the application of best estimate assumptions made in the RRC-A analysis. From discussions with EDF and AREVA, it is apparent that the design change associated with increasing the cooldown rate in response to small break loss of coolant accidents from 100°C/hr to 250°C/hr has resulted in a relaxation of the SG pressure drop trip setpoint, which now means that the low SG level is the most effective trip parameter for these faults. For this reason, Action 2 has been raised with EDF and AREVA as part of the broader GDA Issue on diversity, **GI-UKEPR-FS-02**, to perform an ALARP review into feasibility of providing an additional diverse trip signal or tightening the existing protection setpoints for this fault.

Sensitivity to Two Stuck RCCAs

126 In addition to the additional sensitivities requested for the limiting infrequent steam pipe failure fault, the response to RO-UKEPR-63 (Ref. 43) includes analysis of a more frequent cooldown fault occurring with an assumption of two stuck RCCAs. This was requested because for Sizewell B (Ref. 27) it was known that the probability of two stuck RCCAs was estimated to be 1 x 10^{-5} per demand. Hence, for the more frequent cooldown faults the possibility of two stuck RCCAs cannot be completely ruled out of the design basis given a fault sequence target of 1 x 10^{-7} per year. In response, EDF and AREVA modelled a stuck open MSRT valve sticking open at hot zero power conditions. With two stuck RCCAs, the shutdown margin is reduced to -2380 pcm. The peak return

to power is 3.4% power with a minimum DNBR of 2.71. These results demonstrate that the consequences of such faults are no worse than those for a main steamline break case with a single stuck RCCA discussed above. On the basis of these results, it is judged that the requirements of SAP FA.7 have been met for the case of two stuck RCCAs.

4.2.2.5 Consequential Failures

127 No discussion is presented within the PCSR about the possibility of consequential SGTR failures during a steam line break. For Sizewell B the conditional failure probability for consequential SGTR is assumed to be as high as 1×10^{-1} per demand. Given such high consequential failure probabilities, there is a case for considering whether such sequences should be considered within the design basis for the EPR according to SAPs FA.5 and FA.6. For this reason, TQ-EPR-950 (Ref. 9) was raised requesting EDF and AREVA to provide additional arguments or analysis to justify their position.

128 In their response to the TQ, EDF and AREVA have assessed the consequences of two possible fault sequences covering consequential SGTR. The first fault sequence considers the spurious opening of an MSRT valve. This results in the depressurisation of the secondary side and consequential failure of a single SGTR. The transient is similar to the standard single SGTR fault sequence but with the order of events reversed; the MSRT valve opening causes a consequential SGTR failure rather than in the conventional case where the resultant overpressure transient on the secondary side causes the MSRT valve to lift. The analysis states that no additional single failures are considered but the affected MSRT valve is assumed to remain open and is not isolated. The results are slightly more favourable than the PCC-3 SGTR sequence presented in Ref. 12 in terms of radiological releases to the environment but this is largely due to assumption of operator action after 30 minutes stated in the TQ response. As is discussed in Section 4.2.8 below, EDF and AREVA are proposing to change their safety case for SGTR faults from that presented in Ref. 12. I have not compared directly the radiological releases presented in response to TQ-EPR-950 with any revised PCC-3 SGTR analysis.

129 The TQ response does not consider the possibility of more than one consequential SGTR failure occurring as a result of the transient. In the case of more than one SGTR failure, the reactor will automatically be tripped since the CVCS is not functionally capable of making up the losses due to such breaks. Nevertheless, it is not obvious that the release from the fault is bounded.

130 The second fault sequence considers a main steamline break occurring down stream of the MSIV. Failure upstream is excluded from consideration on the grounds that the main steamline pipework upstream of the MSIV is a break precluded region. The depressurisation of the secondary side is assumed to cause a single SGTR. The secondary side depressurisation transient results in the RPS isolating the MSIV and so the fault effectively transforms into a standard SGTR fault but with an immediate automatic reactor trip. Given that the fault does not assume any additional single failures such as failure of the MSIV to close on demand it is argued that the radiological consequences will be bounded by the normal SGTR fault sequence.

131 This case does not take into account the possibility of more than one consequential SGTR failure occurring as a result of the transient and it also discounts the possibility of the MSIV failing to close as the result of a single failure. Given EDF and AREVA's own PSA gives a sequence frequency of 1×10^{-5} per year for this fault, the additional single

failure needs to be considered as design basis sequence unless it can be bounded by another design basis fault. This has been raised as an Assessment Finding, **AF-UKEPR-FS-05**, for a future operator to respond to during site licensing, once the standard PCC-3 SGTR fault sequence has been clarified during GDA (see Section 4.2.8).

4.2.2.6 Controlled State to Safe Shutdown State

132 EDF and AREVA have considered how to move the reactor from the controlled state to the safe shutdown state. In the case of the steamline break fault, the first action is to isolate the affected SG to prevent a further cooldown, to maintain a low containment pressure and to conserve water in the EFWS tank. The operator then uses the MSRTs to perform a controlled blowdown of the unaffected SGs. Feed to the remaining SGs is provided by the EFWS while the EBS is used to increase the boron concentration in the primary circuit to maintain an adequate shutdown margin. Feedwater supplies from the affected SG can be re-aligned to other SGs should this be necessary. After isolation of the affected SG, EDF and AREVA argue that the situation is essentially identical to that found in the feedwater pipe break case, which is discussed in Section 4.2.3 below. I accept these arguments.

133 EDF and AREVA argue that move from controlled state to safe shutdown state for the other increase in heat removal faults are bounded by the steamline and feedline break cases. This ignores the fact that these events are more frequent and so there is a need to demonstrate a diverse means of reaching the safe shutdown state. This issue has been raised as Action 9 under the GDA Issue, **GI-UKEPR-FS-02**.

4.2.2.7 Radiological Consequence Assessment

134 SAPs FA.3 and FA.7 require that a radiological consequence assessment, on a conservative basis, should be performed for each design basis fault sequence that can lead to the release of radioactive material. A detailed review of the radiological consequence assessment methodology applied by EDF and AREVA to design basis faults is presented in Section 4.3 below. The conclusion of this review is that further substantiation and justification is still required as part of new site specific radiological consequence analyses, but it is my judgement that the current methodology presented in the PCSR (Ref.12) is broadly appropriate for this preliminary Step 4 GDA Assessment of individual faults against Target 4 in the HSE SAPs.

135 The PCSR (Ref. 12) argues that the excessive increase in secondary steam flow (including spurious opening or failure to close of an MSRT) is bounded by the release from loss of condenser vacuum fault. This is also a PCC-2 event and assumes a single failure that results in failure to isolate the MSRT, therefore the steam releases will be equivalent. The releases from the condenser vacuum fault comfortably meet the Target 4 limit. In the case of a main steamline break, EDF and AREVA argue that the radiological consequences are bounded by the release from a PCC-4 two tube SGTR fault. EDF and AREVA have calculated that this latter event gives an off-site dose to an individual of about 2 mSv. Given that the SGTR fault is assumed to result in the direct leak of primary coolant to atmosphere, I judge that the consequences from a main steamline fault will be bounded by this fault. Even if the main steamline break fault resulted in a consequential SGTR fault, I judge that the consequences will not be significantly different from those for the two SGTR fault and the fault frequency will be shifted towards the lower end of the PCC-4 spectrum of frequencies providing DNB can be avoided. As noted above, Action 2 of GDA Issue **GI-UKEPR-FS-02** has been raised requiring EDF and AREVA to

investigate the feasibility of improving protection against this fault. Assuming this is achieved and given the expected frequency for a PCC-4 fault, I am satisfied that the requirements of Target 4 of the SAPs are likely to be met.

4.2.2.8 The Manta Computer Code

136 The MANTA V3.7 computer code is the principal code used by EDF and AREVA to model the thermal hydraulic conditions of the reactor primary and secondary circuits following intact circuit faults including cooldown faults such steamline break faults, heatup faults such as loss of feed faults, flow reduction faults, reactivity and power distribution faults and anticipated transients without trip faults.

137 The physical modelling within MANTA is detailed in Ref. 30 while the main validation evidence is provided in Ref. 31. EDF and AREVA have provided additional information (Refs 32 and 33) to support the validation evidence for the code although one of these (Ref. 33) is not currently referenced from within the PCSR (Ref. 12).

138 The MANTA code represents the flow of liquid and vapour within the primary circuit and the steam generators using a 1-dimensional flow network. The model solves five coupled equations for each control volume, two representing conservation of steam mass and total mass, two representing conservation of energy stored in the steam and liquid phases and one representing the conservation of total momentum. This is complemented by a drift flux model to determine the flow separation between the two phases. Heat transfer between the liquid and vapour phases and the structures within the reactor are represented by empirically derived heat transfer correlations. Empirically derived correlations are also used to determine the wall friction coefficients and critical flow rates for one and two-phase flow and to determine critical heat flux.

139 Given the complex way in which the code integrates all of this empirical information derived from separate effect tests, it is important to validate the code against full and part scale integral tests as required SAP FA.18. The validation work for MANTA is reported in Ref. 31. This presents a comparison of code predictions against a series of experimental tests covering both steady state and transient conditions. Many of the measurements are taken from tests on operational reactors as well as purpose built test facilities. The transients include reactor trip events, a natural circulation test, an overpressurisation test, a secondary side depressurisation test and a feedwater injection test, as well as operational load manoeuvring transients.

140 While the range of tests presented is impressive (four steady state tests, 15 transient tests), only a limited selection of parameters from each individual test is presented for comparison. So although the agreement looks good on the parameters presented, it is difficult to judge how well the code has performed overall against the tests. Furthermore, there is no discussion of how representative the tests are for the UK EPR design. In particular, there are a number of phenomenon (bubble formation in the vessel head, water slug progression, vessel inlet/outlet mixing, natural circulation under solid conditions, heat transfer with degraded inventory, SG dryout or filling, efficiency of flooded moisture separators, auxiliary feedwater performance under degraded conditions) for which only a single test provides the validation evidence for the model. No phenomenon identification and ranking table (PIRT) or scaling analysis is presented within the document to demonstrate that the coverage and relevance of the test results is sufficient to comprehensively validate the MANTA model for application to the UK EPR.

141 For this reason, I decided to select two sample areas for a more detailed assessment of the MANTA validation evidence. The areas selected were the modelling of mixing in the

lower plenum for steamline break faults and the coupling of MANTA, together with SMART and FLICA III, for the performance of coupled thermal hydraulics and 3D reactor physics calculations.

142 The MANTA validation report presents only a single test transient to validate the mixing of flows within the lower plenum (Ref. 31). This involves a test performed at the PALUEL 3 reactor, in which one MSRT valve was opened for five minutes when the reactor was in the hot shutdown state. Feed flow on the effective SG was isolated. Since little information was provided within the MANTA validation report, a copy of the test report (Ref. 32) was requested. This report presents a description of the test transient, the measurements taken, together with a discussion of their uncertainties, the modelling assumptions and the results of the comparison between the test results and the MANTA code predictions including a discussion of the discrepancies. The report notes that the initial test conditions were not well known but claims that this does not jeopardise the validity of the mixing matrix. My own observation is that the sensitivity study performed using an extreme range of mixing assumptions does not seem to particularly affect the quality of the agreement between the test and the MANTA code. This suggests that the test is not very sensitive to the choice of the mixing matrix assumed in MANTA and implies that the test presented is of limited value in terms of validation. There is also no PIRT or scaling analysis to establish how prototypic the lower plenum of the PALUEL 3 plant is compared with that of the UK EPR for validating the mixing phenomenon.

143 Since the PCSR (Ref. 12) was issued, new validation evidence has become available to validate the lower plenum mixing matrices for the UK EPR based upon the Juliette test rig (Ref. 33). The Juliette rig is a 20% scale model of the lower plenum of the UK EPR including the four cold leg inlet pipes and nozzles, the reactor annulus, the vessel bottom head, the flow distribution device and core support structure and outlet shell. The validation report (Ref. 33) describes the Juliette mock-up, interprets the test results, derives best estimate mixing matrices by comparison of MANTA predictions with Juliette results and recommends penalised mixing coefficients for fault analysis purposes, including penalising mixing matrices for MANTA and zoning matrices for use with FLICA III. These revised matrices have been used in the analysis performed in the response to RO-UKEPR-63 (Ref. 43). I judge the work reported to have been performed to an excellent standard. However, it should be noted that the Juliette tests were performed in isothermal conditions and are only valid for forced circulation flows. Hence, they cannot be used when buoyancy effects and natural circulation flows are dominant. Furthermore, the work has not been captured within the MANTA validation report (Ref. 30) and illustrates that the validation report is out of date and in need of revision.

144 An Assessment Finding, **AF-UKEPR-FS-06**, has been raised requiring a future licensee to review the MANTA validation report to see whether there are any further updates that are required in the report. In particular, they will be asked to perform a PIRT (Phenomena Identification and Ranking Technique) and scaling analysis to demonstrate that the validation evidence is appropriate for the UK EPR, particularly where this consists of singleton tests. Should any gaps in the supporting validation be identified, the future licensee will be requested to make proposals on how additional evidence can be generated. In addition, the operator will be requested to identify whether there are any commissioning tests that would aid code validation. For example, on Sizewell B, commissioning tests were performed to help with the validation of mixing coefficients in the lower plenum. As noted above, in Section 4.2.2.3, the future licensee is also required under Assessment Finding **AF-UKEPR-FS-01** to present its validation evidence for lower plenum mixing following tripping of the RCPs.

145 Although the MANTA code is provided with a point-kinetics model, as noted above, it can also be used with the SMART 3-D reactor kinetics code and the FLICA III sub-channel code to perform coupled thermal hydraulic and reactor physics calculations. This methodology is applied primarily for analysis of the steamline break, RCCA ejection faults and for the analysis of ATWT events. The validation evidence (Refs 28 and 29) for the veracity of the coupling scheme essentially rests upon a comparison of standalone calculations performed with the individual codes benchmarked with those performed using the coupled method, although EDF and AREVA were able to present analysis of RCCA drop events performed using the SMART and FLICA III codes coupled together. The general lack of experimental data from an integral test to provide validation evidence to support the MANTA, SMART, FLICA III coupling scheme is undesirable and for this reason the future licensees are requested, under Assessment Finding **AF-UKEPR-FS-07**, to demonstrate the performance of the codes against an international benchmark exercise such as a boiling water reactor stability benchmark (Ref. 47) or other suitable test data agreed with the regulator. This should provide a good test of the codes for conditions close to saturation, that are representative of those that would be found during faults such as an ATWT or steamline break event and is consistent with the thinking behind SAPs FA.18 and FA.22.

146 Given the importance of this coupled code scheme within the design basis safety analysis for the UK EPR, I decided it was necessary to perform confirmatory analysis for the main steamline break fault (see above), the loss of feed ATWT event (Section 4.2.3), and the loss of flow ATWT event (Section 4.2.5).

147 On the basis of the above discussion, it is considered that further validation evidence is required for the MANTA code to fully meet the requirements of SAPs FA.17 to FA.19 and FA.21 to FA.22. Nevertheless, it is recognised that the physical principles of the code are soundly based and the confirmatory studies performed by GRS in Sections 4.2.2, 4.2.3, and 4.2.5 are judged to be totally supportive of the MANTA predictions such that the further work to be performed under Assessment Finding **AF-UKEPR-FS-07** is considered unlikely to identify any shortfalls in the code. During GDA Step 4 no assessment has been made of the quality assurance procedures controlling the development, maintenance and application of the MANTA code against SAP FA.20. In addition, no assessment has been performed against SAP FA.23 on data collection and SAP FA.24 on the periodic review and update of fault analysis. HSE ND may elect to perform such assessments during the site licensing process.

4.2.2.9 Findings

148 Following my assessment of increase in heat removal faults, I am broadly content with the fundamental design of the UK EPR to protect against this class of fault. It is judged that the large shutdown margin on the UK EPR provides significant protection against these faults and largely compensates for the move away from a high head to medium head safety injection system. I also welcome the decision by EDF and AREVA to automate the initiation of the EBS on the low SG pressure signal.

149 My only remaining concern is on the adequacy of the protection system to protect against those faults that result in intermediate cooldown rates with the reactor at full power. The protection appears slow to respond to these faults. These faults are potentially frequent and so this concern carries over to the diverse protection system and for this reason Action 2 has been raised under the GDA Issue on diversity, **GI-UKEPR-FS-02**, to review the protection provided.

150 In addition, seven Assessment Findings have been raised (**AF-UKEPR-FS-01** to **AF-UKEPR-FS-07**). In general, these are items requiring either further analysis or support from commissioning tests rather than a fundamental issue with the design and, in my judgement, they can be closed out as part of the site licensing process.

4.2.3 Decrease in Heat Removal Faults

4.2.3.1 Summary of EDF and AREVA's Safety Case

151 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, thereby 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 LOCA.

152 The basis of EDF and AREVA's 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 RPS is able to trip the reactor and initiate adequate post-trip cooling using the EFWS and MSRT system. They also conclude that the MSSVs provide adequate overpressure protection for this class of faults.

153 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 performed 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 so as to threaten the structural integrity of the primary circuit.

4.2.3.2 Assessment (Overview)

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

- spurious turbine trip;

- loss of condenser vacuum;
- short term loss of offsite power (≤2 hours);
- long term loss of offsite power (> 2 hours);
- loss of main feedwater flow;
- inadvertent closure of main steam isolation valves; and
- feedwater system pipe break.

155 All the above events are considered to be PCC-2 events, with the exception of the long term LOOP for greater than two hours and the inadvertent closure of the main steam isolation valves which are considered PCC-3 events 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 main 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.

156 My assessments of the three sampled faults are presented separately in the sections below. Section 4.2.3.3 discusses feedwater system pipe break, Section 4.2.3.4 discusses inadvertent closure of the main steam isolation valves and Section 4.2.3.5 discusses loss of main feedwater flow. I have also commented in the subsequent sections on EDF and AREVA's safety case for consequential failures, achieving safe shutdown and the assessed radiological consequences from decrease in heat removal faults.

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

Fault Sequence Analysis

157 The feedwater system piping failure assessment assumes the rupture of a main feedline. 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.

158 EDF and AREVA have indeed treated the fault as within the design basis, meeting the requirements of SAPs FA.3 and FA.4 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 PSVs 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. During GDA Step 4, EDF and AREVA have provided arguments that these are covered by the PCC-3 design basis event, inadvertent opening of a pressuriser safety valve case. These arguments are discussed further below in the section on consequential failures (Section 4.2.3.6).

159 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 of 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 accept these arguments.

Methods and Assumptions

160 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling this feedwater system pipe break, EDF and AREVA have made the following assumptions to ensure a robust and conservative assessment.

- A pessimised power level of 102% and a decay heat pessimised to the 95% confidence level are assumed.
- No reactor trip signal arising on the primary side is claimed.
- No reactor trip signal arising on the affected SG is claimed.
- For the large double-ended guillotine break of the feedline assumed in the analysis presented in the PCSR, the reactor would trip either on high SG pressure drop or low SG pressure rather than the low SG level trip actually claimed. This is to cover the full spectrum of feedline break sizes but results in a conservative estimate of SG water inventory for the case analysed.

161 These assumptions represent a standard approach to the design basis analysis of such faults and are comparable to those applied in the equivalent Sizewell B analysis. They are judged to result in a bounding assessment meeting the requirements of SAP FA.7.

162 The EDF and AREVA analysis uses the CATHARE computer code to model this feedwater system pipe break. The THEMIS and FLICA codes are used to model the MSIV closure transients discussed below while the overpressure analysis aspects of this fault (reported in Chapter 3.4 of the PCSR) uses the MANTA code. The assessments of the validation evidence for the MANTA and CATHARE codes against SAPs FA.17 to FA.22 are presented in Sections 4.2.2.8 and 4.2.8.9 respectively in this report, while the FLICA code is assessed separately in the Fuel and Core Assessment Report (Ref. 15). The validation evidence in support of the THEMIS code has not been assessed during GDA Step 4. This is because the analysis performed using this code is gradually being replaced by analysis performed using the MANTA code.

Transient Analysis

163 SAP FA.7 requires that the analysis should demonstrate, so far as is reasonably practicable, that none of the physical barriers to prevent the escape of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact

and without a threat to its integrity. In practice, for faults considered in this section, the aim of EDF and AREVA is to demonstrate this is achieved by ensuring the fuel cladding does not undergo DNB and that the primary circuit does not become water solid threatening the integrity of the primary circuit pressure boundary. To confirm that these objectives have been achieved, the results of design basis analysis of EDF and AREVA for these faults are reviewed.

164 The results of the EDF and AREVA analysis are summarised in Figure 8 of Chapter 14.5.3 of the PCSR (Ref. 12). This presents the pressuriser pressure transient as calculated by EDF and AREVA using the CATHARE computer code for the feedline break fault. The calculations are for a 4250 MWth design of EPR. Similar analysis for a 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. Although this is judged adequate for the purposes of the GDA assessment, clearly over time it is desirable to update the analysis with the UK EPR specific analysis. For this reason, Assessment Finding **AF-UKEPR-FS-08** has been raised requesting a future operator to gradually update the PCSR analysis during the site licensing process with UK EPR specific analysis.

165 The analysis presented assumes the loss of a single EFWS pump 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 while a third EFWS pump is lost as a consequence of the feedline break. The resultant pressuriser pressure transient shown in Figure 8 of Chapter 14.5.3 of the PCSR (Ref. 12) 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 feedwater system pipe break reducing the amount of heat taken out by the SGs. This causes the primary circuit to heat-up until the reactor is tripped on low SG water level. The rise in peak pressure is sufficient to cause the PSVs to open. Following reactor trip, the primary circuit cools and the PSVs close. The remaining available SG also starts to dry out. This causes the second peak in the primary pressure as the circuit heats up again. The PSVs 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 SG water level.

166 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 TQ-EPR-346 (Ref. 9), 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 SG is 25 kg/s (90 te/h) at these fault conditions. EDF and AREVA have confirmed that the need for operator action could be just avoided if the flow from the EFWS pumps was to be increased to 33 kg/s (120 te/h). To provide sufficient heat removal capability to match the heat input from the primary circuit, so as to avoid SG dryout at thirty minutes, would require the flow from the EFWS pumps to increase to 44 kg/s (158 te/h). The auxiliary feedwater flow from a single pump to a pair of SG on Sizewell B (Ref. 48) 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. It is also informative to

perform an additional hand calculation for the heat balance at one hour. At this time the reactor decay is about 1.5% or 68 MW. The RCPs contribute another 30 MW. The operational SG will be held at a pressure of 97 bara by the MSRT. Assuming feed enters at a temperature of 50°C then the enthalpy rise to saturated steam is 2731 kJ/kg - 210 kJ/kg = 2521 kJ/kg. Therefore the heat removal capacity of one SG is 2521 kJ/kg x 25 kg/s = 63,035 kW = 63 MW. Hence, with the RCPs still operational, the heat input of 98 MW greatly exceeds the heat removal capability of one SG. However, if the RCPs are tripped, heat balance has almost been achieved after one hour and will be achieved shortly as the decay heat reduces with time. In contrast, a single MSSV is capable of passing 160 kg/s (575 te/h) at 100 bara, which is more than enough capacity to provide adequate levels of post-trip cooling. A single MSRT valve has twice the capacity of an MSSV.

167 In the case of Sizewell B, most safety systems are provided with four-fold redundancy. The design basis assumption (Ref. 48) 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 is an exception to this principle and it is associated with the feedwater system pipe break fault. The four auxiliary feedwater lines to the SGs are paired together into two common headers. This is done to increase the reliability of the system for loss of feed faults other than the feedline break fault. Sizewell B therefore requires feed from 2-out-of-4 auxiliary feedwater pumps (Ref. 48) to ensure adequate post-trip heat removal following a feedline break fault (there is a second exception; minimum heat removal requirements following an ATWT event which is for 3-out-of-4 trains of the auxiliary feedwater system to be available but this is a low frequency sequence for which the single failure criteria does not apply). 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.

168 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 or to trip the RCPs. In effect, both reactor designs are making a probabilistic argument to exclude the need to consider an additional preventative maintenance given the initiating frequency for the feedline break fault. Although my preference would have been to slightly increase the size of the EFWS pumps, given the ALARP precedent set by Sizewell B, it is judged disproportionate to make EDF and AREVA increase the flow capacity of the EFWS pumps on the UK EPR. Furthermore, it must be recognised that there is no cliff edge in the consequences should the pressuriser go water solid since the PSV valves are qualified to pass liquid coolant. Should they fail to re-close this will result in a consequential loss of coolant accident (discussed below) and for which other safeguards are available. Indeed, given the provision of this extra diversity, it could be argued that the single failure criteria should not be applied to one of the EFWS pumps. With 2-out-of-4 trains available, the EFWS pumps have sufficient capacity to remove all the decay heat without the need for the pressuriser to go water solid such that the design meets the requirements of SAPs FA.6, EDR.2 and EDR.4. However, it should be noted that there is scope for a potential ALARP measure to temporarily reduce the reactor power when one EFWS pump is put into maintenance such that 1-out-of-4 EFWS pumps would provide adequate heat removal. For this reason, Assessment Finding **AF-UKEPR-FS-09** has been raised requiring a future licensee to perform a quantitative ALARP assessment as to whether an EFWS train should be maintained while at power.

Subject to this finding, it is judged that the requirements of SAP FA.7 have been met for the feedline break fault.

4.2.3.4 Assessment of Inadvertent Closure of all MSIVs (Limiting Frequent Fault - Overpressurisation)

Fault Sequence Analysis

169 The inadvertent closure of all four 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 x 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 PSVs. In my Step 3 Assessment Report, I noted that this contrasts markedly with the situation at Sizewell B which is provided with three Pilot Operated Safety Relief Valves (POSRV) and a diverse set of two spring loaded Pressuriser Safety Relief Valves (PSRV). 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 probability of failure 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.

170 The analysis for these faults is presented within Chapter 14.4 of the PCSR (Ref. 12). 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 (Ref. 12) 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 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 RPS 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 judged to be acceptable. The UK EPR design also provides for the isolation of the MSRT valves which is probably an advantage for cooldown faults discussed earlier and the SGTR faults discussed in Section 4.2.8. However, on the primary side there appears to be no diverse safety system to protect against the common mode failure of the PSVs. Given that this event is considered to be frequent, EDF and AREVA were required to review this fault as part of RO-UKEPR-41 (Ref. 10) in order to demonstrate functional diversity.

171 In their response to RO-UKEPR-41 (Refs 45 and 46), EDF and AREVA have identified the need to study two fault sequences following an inadvertent closure of all MSIVs event. The first case is due to common mode failure of the PSVs to open on the primary side. The second is due to common mode failure of the MSRTs to open on the secondary side.

Transient Analysis

172 For the case of inadvertent closure of all MSIVs with common mode failure of the PSVs, the closure of all the MSIVs causes an increase in the pressure of the secondary system. As a consequence, the heat removal capability is reduced and this causes the temperature and pressure of the primary system to increase resulting in a reactor trip on high pressuriser pressure. This causes the main feed to be tripped. However, on the primary side the PSVs are assumed to fail to open and the primary pressures reaches a peak pressure of 209.3 bara (for the sensitivity case where the pressuriser spray is also assumed to fail) before the opening of the MSRT valves on the secondary side starts to restore heat removal from the primary side. The analysis demonstrates that the peak pressure is significantly below the primary pressure limit of 228 bara applicable for such low frequency events. The analysis conservatively models the MSIVs valves closing with a stroke time of 0.1 second and uses conservative values for the initial reactor power and reactor protection trip setpoints. Conservative values are used for relief capacity of the MSRT valves.

173 This is an important transient since it demonstrates that the pressuriser has been sized sufficiently large to enable the plant to "ride-out" the transient without the need for the diverse set of spring loaded safety relief valves that are provided on the Sizewell B design. The predicted pressure rise implies that the steam bubble in the pressuriser is reduced in size by about 25%. A 31% reduction would have eroded the safety margin. A study of the MANTA validation report (Ref. 31) suggests the filling and draining of pressuriser, the so called "piston effect", is validated by three tests. Two of these tests (CRUAS 2, BUGEY 4) show good agreement with the MANTA code predictions. In the third test, the rise in pressuriser level in the GRAVELINES 6 test appears to be underestimated by about 3%. However, there are some uncertainties associated with the test conditions. Overall, my judgement is that an adequate demonstration has been provided for the purposes of this GDA assessment to meet the requirements of SAP FA.7. However, there is scope to improve the validation evidence for the MANTA code with regard to this phenomenon further during commissioning tests on the EPR. As noted in Section 4.2.2.8 above, future licensees have been requested to review the scope for using commissioning tests to provide additional validation evidence for the MANTA code under Assessment Finding **AF-UKEPR-FS-06**.

174 The case of inadvertent closure of all MSIVs with common mode failure of the MSRTs, the closure of all the MSIVs causes an increase in the pressure of the secondary system as in the previous case. The transient initially proceeds identically with the previous case until the PSVs successfully open limiting the primary pressure which peaks at 187.6 bara. The MSRTs fail to open causing the secondary side pressure to rise to 108.7 bara, only slightly above the MSSV setpoint of 106.5 bara and comfortably below the design pressure of 129.7 bara. Given the capacity of a single MSSV is 25% of full flow, it is not surprising that two MSSVs are capable of controlling the secondary side pressure once the reactor is tripped. Indeed, this transient is bounded by the analysis reported in Chapter 3.4 of the PCSR, which assumes the failure of the all MSRTs and an additional single failure of a MSSV. In my judgement, the requirements of SAP FA.7 have been met.

4.2.3.5 Assessment of Loss of Main Feedwater (Limiting Frequent Fault – Decay Heat Removal)

Fault Sequence Analysis

175 Although EDF and AREVA have identified that the loss of main 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 feedwater system pipe break fault discussed above. The only significant difference is that all four SGs are intact and so they all contain water during the early stages of the transient. In my GDA Step 3 Assessment Report, I noted that, unless EDF and AREVA are arguing that two EFWS pumps are available for cooling (after assuming one pump is unavailable due to preventive 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 SGs is only likely to delay the transient compared with the feedwater system pipe break case. It will not eliminate the possibility of SG dryout or significantly alter the margin to fill on the pressuriser water level if only one EFWS pump is available. EDF and AREVA have confirmed in TQ-EPR-683 (Ref. 9) that they do need 2-out-of-4 EFWS pumps to be available to ensure that the pressuriser does not go water solid. During GDA Step 4, EDF and AREVA were requested to consider the feasibility of increasing the sizing of the EFWS pumps recognising that a 2-out-of-4 system will have a lower reliability than a 1-out-of-4 system.

176 From a systems perspective, EDF and AREVA are effectively claiming (TQ-EPR-683, Ref. 9) that the UK EPR has three diverse feed systems; the two EFWS pumps in divisions 1 and 4 of the safeguard buildings which provide feed for two of the SGs, the two EFWS pumps in divisions 2 and 3 of the safeguard buildings which provide feed for the remaining two SGs, and bleed and feed using the safety injection system that requires manual operation to depressurise the reactor. To ensure functional diversity, the two EFWS pumps on divisions 1 and 4 are supplied by a low voltage (690 V) system while the two EFWS pumps on divisions 2 and 3 are supplied by a high voltage (10 kV) system. The motive power for the EFWS pumps is taken from the alternating current (AC) essential electrical system which is backed up by four emergency diesel generators (EDG) should there be a LOOP in coincidence with the reactor trip. In addition, to ensure functional diversity, two manually operated Station Blackout (SBO) diesels are provided for the two EFWS pumps in divisions 1 and 4 should the EDGs undergo a common mode failure. These need to be started within 1.5 hours of the start of the fault.

177 In their response to TQ-EPR-683 (Ref. 9) EDF and AREVA estimate that the current design of EFWS pumps are capable of achieving the desired flow rate for a 1-out-of-4 system. However, the increased power requirements could not be provided by the current design of SBO diesels. Furthermore, EDF and AREVA consider that changing the specification of the SBO diesel generators would necessitate alterations to the design of the civil structures of the diesel houses. From a design basis perspective, it has to be recognised that there is no justification for requiring a design change providing that the loss of feedwater fault is not capable of causing a consequential failure of one of the four EFWS trains, since the single failure and preventative maintenance requirements in SAPs FA.6, EDR.2 and EDR4 are meet by a 2-out-of-4 system.

178 Although these SBO diesels are of a diverse design to the four main EDGs, they are clearly not as functionally diverse as the steam driven auxiliary feedwater system provided on Sizewell B which is driven by steam stored in the SGs. However, it is accepted that there are precedents for all electrically powered reactors in the UK. The power stations at Heysham 2 and Torness are built to modern standards and are all

electrically powered (although it must be noted that the timescales for restoration of electrical power are longer on AGRs because of their high thermal inertia). Furthermore, it is the view of EDF and AREVA, based on reliability data from EDF's fleet of operating reactors (TQ-EPR-951, Ref. 9) that steam driven pumps are less reliable than electrical driven pumps. While my preference would have been for a diverse set of steam driven feed pumps, I judge that it would be disproportionate to insist on a design change given the massive impact it would have on the civil design of the reactor.

179 These considerations emphasised the importance of ensuring that the functional diversity between the EDGs and the SBO diesel generators and the EFWS pumps in divisions 1 and 4 from those in divisions 2 and 3 is not compromised during maintenance activities. It is important that maintenance procedures take account of these diversity requirements by ensuring that the same personnel are not involved in the maintenance of systems that are intended to be diverse and that supplies of diesel oil are provided from diverse sources. For this reason, Assessment Finding **AF-UKEPR-FS-10** has been raised requiring a future operator to develop appropriate arrangements for the maintenance of these diverse systems during the site licensing process.

180 Loss of normal feedwater is a frequent event and so EDF and AREVA have reviewed the fault in their response to RO-UKEPR-41 in order to demonstrate functional diversity. In their response to RO-UKEPR-41 (Refs 45 and 46), EDF and AREVA have identified the need to analyse the following four fault sequences:

- loss of main feedwater fault with failure of the control rods to insert following reactor trip;
- loss of main feedwater fault with failure of the RPS to initiate a reactor trip signal;
- loss of main feedwater fault with common mode failure of the RCPs; and
- loss of main feedwater fault with common mode failure of the EFWS.

181 My assessments of EDF and AREVA's analysis of these fault sequences are presented below.

Loss of Main Feedwater with ATWT Due to RCCAs Failing to Insert

182 In the case of the loss of main feedwater fault with failure of the RCCAs to insert, the risk reduction feature that has been introduced to provide protection is 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 the low-2 SG level signal is received. This strategy differs from that applied at Sizewell B, which is 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 RCPs, will provide adequate protection for such faults given the inherent characteristics of the moderator temperature coefficients on PWRs.

183 The analysis reported in their RO-UKEPR-41 response (Ref. 46) is performed on a conservative basis consistent with design basis assumptions and so BOC conditions are chosen with the moderator temperature coefficient set at -13.2 pcm/°C. The core power is assumed to be at 102% and the thermal hydraulic design flow rate is chosen. The flow capacities of the PSVs are penalised as are the trip setpoints and signal time delays. The identified design limits to avoid are pressurising the reactor vessel above 228 bara

and a minimum DNBR below 1.21. The analysis is performed with the MANTA, SMART, and FLICA III coupled code analysis route discussed in Section 4.2.2.

184 The results presented (Ref. 46) show that as the SGs empty due to the loss of feedwater, the pressure and temperature in the RCS start to increase. After 32 seconds a reactor trip signal is generated on high pressuriser pressure but the RCCAs are assumed to fail to insert although the turbine is tripped. The pressure continues to increase until two of the PSVs open at 37 and 39 seconds respectively. The ATWT signal is generated 20 seconds after the reactor trip signal actuating the EBS. The decrease in moderator density causes the reactor power to reduce. The PSVs re-close. As the SGs continue to empty the RCPs are also tripped at 86 seconds. This causes an increase in the voiding of the core resulting in a rapid reduction in core power. The EFWS is also actuated at 110 seconds on low SG level. After 600 seconds the boron injected from the EBS enters the core and the reactor is shutdown. Although the primary system goes water solid, the flow capacity from just one of the three PSVs valves is sufficient to keep the pressuriser pressure below 177 bara. Although the peak pressure in the primary circuit will be about 10 bar higher, this is still well below the structural integrity limit of 228 bara. The rise in pressure is sufficient to ensure adequate margin to DNB. These results suggest that adequate protection is provided for this fault sequence meeting the requirements of SAP FA.7 and that there is no need for a fast acting EBS as provided at Sizewell B.

185 In addition to the analysis performed in response to RO-UKEPR-41, EDF and AREVA have also calculated this transient within the RRC-A sequence analysis reported in Chapter 16.1 of the PCSR using a best estimate analysis. The analysis confirms that although the reactor goes water solid, the flow capacity from a single PSV (analysed using the previous SEBIM design of valve rather than the latest SEMPELL valve) is sufficient to keep the pressuriser pressure below about 177 bara and the primary pressure below about 187 bara. This case is reported because it has been used as a benchmark case for some confirmatory analysis performed by GRS.

Confirmatory Analysis

186 GRS has repeated the RRC-A loss of normal feedwater ATWT case using its own ATHLET systems code and its own 3D QUABOX/CUBBOX reactor kinetics code coupled together. The results of its comparison (Ref. 49) show good agreement with EDF and AREVA's predictions recognising that the GRS calculations assume a different moderator temperature coefficient due to a lower initial boron concentration, which will ensure a more negative temperature coefficient. The expected pressure rise for the GRS results should therefore be slower than the EDF and AREVA's predictions since the reactor power will fall quicker for a given temperature rise. The GRS analysis also models the latest SEMPELL valves.

187 The secondary side predictions are very similar. Primary side temperatures are also in good agreement. The GRS power level falls of quicker, as expected. The main difference is in the pressure response and the flow through the PSVs. However, I have compared the GRS predictions with the RO-UKEPR-41 predictions for this sequence (Ref. 46) which also models the latest SEMPELL valves and the timings and the shape of the pressure response is much closer to the more recent RO-UKEPR-41 predictions than the RRC-A analysis. The vapour flows are virtually identical. The liquid flow transients are also similar although the GRS flows are about 150% greater. This is likely to be because GRS are performing a best estimate analysis while EDF and AREVA have conservatively penalised the flow rates through the PSVs in their analysis. Given that the

results are effectively blind comparisons, since neither EDF and AREVA nor GRS have seen each other's results, I judge that the agreement to be very good.

188 The comparison has improved my confidence in the EDF and AREVA analysis. In my judgement, the requirements of SAP FA.7 have been met. In particular, there is no need to require EDF and AREVA to install a fast acting emergency boration system on the UK EPR on the basis of this comparison. I therefore judge the requirements of RO-UKEPR-62 (Ref. 10) have been met through the response to RO-UKEPR-41 (Ref. 46).

Loss of Main Feedwater with ATWT Due to RPS Failure

189 In the case of the RPS failing to trip the reactor following a loss of main feedwater fault, EDF and AREVA are proposing a design change. They are introducing a new trip signal to be fitted on a diverse protection system to trip the reactor on high pressuriser pressure under modification CMF#23 (Ref. 42). Previously, 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 SG level signal. EDF and AREVA have not yet confirmed whether the new high pressuriser pressure trip will be on the PAS/SAS or the non-computer based safety system (NCSS). Either system will reduce the time until reactor trip occurs (compared to a SG level trip) which is a positive development from a safety perspective.

190 The analysis reported in their RO-UKEPR-41 response (Ref. 46) is performed on a conservative basis, consistent with design basis assumptions including BOC conditions with the moderator temperature coefficient set at -13.2 pcm/°C. The core power is assumed to be at 102% and the thermal hydraulic design flow rate is chosen. The flow capacities of the PSVs are penalised as are the trip setpoints and signal time delays. The identified design limits to avoid are pressurising the reactor vessel above 228 bara and a minimum DNBR below 1.21. The analysis is performed with the MANTA, SMART, and FLICA III coupled code analysis route discussed in Section 4.2.2 up until the time of trip. After reactor trip, the MANTA code is used with its point kinetics model.

191 The results presented (Ref. 46) show that as the SGs empty due to the loss of feedwater, the pressure and temperature in the RCS start to increase. Unlike the previous fault sequence, no reactor trip signal is generated on high pressuriser pressure due to assumed failure of the RPS. Instead, the reactor trip signal is generated on proposed high hot leg pressure on the diverse reactor protection system after 60 seconds. The pressure continues to increase until one of the PSVs open at 61.5 seconds. It re-closes at 84 seconds. As the SGs continue to empty, the RCPs are also tripped at 720 seconds. The primary system goes water solid but the flow capacity from just one of the three PSVs valves is sufficient to keep the pressuriser pressure below 174 bara. Although the peak pressure in the primary circuit will be about 10 bar higher, this is still well below the structural integrity limit of 228 bara. As in the previous case, the rise in pressure is sufficient to ensure adequate margin is maintained to DNB. However, a significant difference to the previous sequence is that the EFWS is not actuated because the RPS is unavailable. EDF and AREVA argue that after 30 minutes the operator can start the EFWS pumps or commence bleed and feed operations.

192 Without operator action, the position at the end of 30 minutes does not represent a controlled state. On the secondary side, the SGs have dried out. On the primary side, temperatures are approaching saturation conditions and the reactor is water solid with an open PSV, such that the primary liquid mass is falling rapidly.

193 These results have been discussed with EDF and AREVA. In response, they have informed HSE ND that they are in the process of developing proposals to automate the actuation of the EFWS system on very low SG pressure within the design modification being implemented under CMF #14 for the NCSS. In their response to TQ-EPR-1432 (Ref. 9), EDF and AREVA have performed transient analysis to demonstrate the effectiveness of the modification, although the results were received too late to be included in the revised version of the PCSR (Ref. 14). In my judgement, this is a major safety improvement and its implementation is fully supported. Implementation of this modification and updating of the PCSR with these results will be closed out under GDA Issue **GI-UKEPR-CC-02**. Implementation of the hot leg pressure trip and the EFWS actuation on very low SG level modifications on the diverse protection system is being covered under GDA Issue **GI-UKEPR-FS-02** on diversity (Action 1). Given these important commitments, it is my judgement that the intended protection provided for this fault sequence should meet the requirements of SAP FA.7.

Loss of Main Feedwater with Common Mode Failure of the RCPs

194 EDF and AREVA have considered RCP trip occurring with loss of normal feed. The loss of the main and stand-by feed results in the EFWS being actuated to provide feed to the SGs. The tripping of the RCPs results in natural circulation cooling of the primary circuit. Without claiming the normal control systems, the reactor pressure rises and results in one PSV opening. The reactor is tripped on low SG level. In my judgement, this is a non-limiting transient.

Loss of Main Feedwater with Common Mode Failure of the EFWS (Bleed and Feed)

195 EDF and AREVA have considered the total loss of feedwater case in which loss of main feedwater is assumed to occur together with the common mode failure of the EFWS pumps in safeguard divisions 1 & 4 as well as common mode failure of the EFWS pumps in safeguard divisions 2 & 3. The analysis reported in their RO-UKEPR-41 response (Ref. 46) is performed on a conservative basis consistent with design basis assumptions and so the core power is assumed to be at 102% and the thermal hydraulic design flow rate is chosen. The decay heat is assumed at the 95% confidence level. A partial trip function on the RCSL is claimed to reduce the reactor power to counteract the power mismatch between the primary and secondary system. EDF and AREVA have classified this as an F2 function. However, it is understood that they have agreed that the RCSL is to be a Class 2 system so this is considered to be acceptable. Operator action is claimed after 30 minutes to switch off the pressuriser heaters. After 2935 seconds the operator is assumed to perform the bleed and feed operation using the Primary Depressurisation System (PDS) on the basis of the core exit temperature exceeding 330°C. The PDS is identified as fulfilling an F2 function and so EDF and AREVA need to justify that the PDSs meet the requirements for a Class 2 system under Action 5 of **GI-UKEPR-CC-01**. This action, together with the manual actuation of the safety injection system (SIS), takes the reactor to the controlled state. The analysis is performed with the CATHARE 2 V2.5 code discussed in Section 4.2.8.

196 The results presented (Ref. 46) show that as the SGs empty due to the loss of feedwater, the pressure and temperature in the RCS start to increase. After five seconds the partial trip occurs and the turbine is tripped causing the reactor to trip 10 seconds later. After 978 seconds the SG blowdown is isolated. The pressuriser heaters are switched off by the operator at 1815 seconds. As the SGs continue to empty the RCPs are also

manually tripped at 1852 seconds. The pressure continues to increase until one of the PSVs opens at 2557 seconds. At 2935 seconds the core outlet temperature reaches 330°C and the operator starts bleed and feed operations. The operator is also assumed to perform a partial cooldown on the secondary side. The consequential rapid depressurisation allows the MHSI and accumulators to inject. The results essentially show that, providing bleed and feed is commenced before or at about the time of SG dryout, then the fuel clad does not experience a loss of cooling. The time for operator action is 55 minutes which meets the requirements of SAP ESS.9 with regards to the 30 minutes rule. Nevertheless, bleed and feed is being claimed within the design basis and so it is important that the operators are well trained for these operations.

197 The total loss of feedwater case including the common mode failure of all the EFWS is also presented as a risk reduction sequence in the RRC-A analysis in Chapter 16.1 of the PCSR but for the 4250 MWth design. 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 systems such as the CVCS letdown and charging systems. In addition, two single failures are considered. These are that one of the PSVs fails to open (case 1) and one of the MHSI trains fails to operate (case 2). In addition, operator action is not claimed for the first 30 minutes.

198 These cases are more informative in that EDF and AREVA delay the time at which bleed and feed operations commence until the RCS level reaches the low loop level setpoint (at 9500 seconds or 2.6 hours for case 2). Use of the letdown system appears to delay the time to the first PSV opening to 5700 seconds. The primary circuit has reached saturation conditions and the liquid mass is significantly more depleted at the time when bleed and feed operation commences. Opening the PDS results in the temporary loss of cooling to the fuel rods until the water inventory is replenished by the MHSI. The average rod temperature peaks at 500°C (case 1). I estimate that the hot rod temperature will be about 650°C, so this suggests that even for the hottest rod there is a large margin to the clad melt temperature of 1200°C. Clad ballooning is also not a concern at these temperatures. The decay heat at this time will be about 44 MW which is consistent with a clad temperature gradient of about 0.5°C/s during the heat-up phase. Delays of the order 300 seconds in restoring cooling would be needed to have a significant effect on the predicted peak clad temperature.

199 On the basis of the analysis presented by EDF and AREVA, the sizing of the PDS valves appears to be adequate to ensure a rapid depressurisation of the primary circuit over about 900 seconds. This is sufficient to get the MHSI and accumulators injecting early enough to limit the peak clad temperature. Although the calculation has been performed using the RRC-A methods and assumptions, my judgement is that the results will only be affected by about 80°C using the design basis methodology assumed in the RO-UKEPR-41 response with decay heat at the 95% confidence level. On this basis, I judge that the requirements of SAP FA.7 have been met subject to the human factors assessment concluding that the bleed and feed operation can be performed on a timescale of the order of two hours with the high reliability (i.e. 1 x 10^{-3} per demand) consistent with that expected of protection for a design basis event. This has been raised as a GDA Issue, **GI-UKEPR-HF-01**, in the Human Factors Assessment Report (Ref. 54).

4.2.3.6 Consequential Failures

200 In my GDA Step 3 Assessment Report, I noted that no discussion was presented within the analyses about the possibility of consequential failures such as a stuck open PSV

failing to close resulting in a consequential LOCA or SGTR failures following a feed line break. I stated that this was 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 TQ-EPR-386 (Ref. 9), it was understood that the conditional failure probability for a PSV failing to close having opened is assumed in the PSA to be 2.5×10^{-2} per demand, and so there was 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. For this reason, TQ-EPR-947 was raised requesting EDF and AREVA to provide additional arguments or analysis to justify their position.

201 In their response to TQ-EPR-947 (Ref. 9), EDF and AREVA have reviewed all the PCC faults that are associated with intact circuits and which could result in the lifting of the PSVs. The events considered are turbine trip, loss of condenser vacuum, LOOP, uncontrolled RCCA bank withdrawal, small steam or feedwater piping failure, inadvertent closure of all four MSIVs, RCCA ejection accident and RCP seizure and shaft break. EDF and AREVA argue that all these events are bounded by the small break LOCA fault since the reactor is tripped in response to the initiating event before the valve has chance to fail in the open position. They also perform the transient analysis for the LOOP case. Essentially, all the plant parameters are unchanged from the nominal conditions apart from the power level which is tripped and the pressure which is slightly higher. The later two effects are beneficial in terms of DNB. I accept these arguments.

4.2.3.7 Controlled State to Safe Shutdown State

202 EDF and AREVA have considered how to move the reactor from the controlled state to the safe shutdown state. In the case of the feedline break fault, this is achieved by the operator using the MSRTs to blowdown the unaffected SGs after tripping two of the four RCPs. Feed to the affected SG is isolated. Feed to the remaining SGs is provided by the EFWS, while the EBS is used to increase the boron concentration in the primary circuit to maintain an adequate shutdown margin. The MSIV bypass line is available should a single failure disable the MSRTs. Feedwater supplies from the affected SG can be re-aligned to other SGs should this be necessary. The worst preventative maintenance and single failure are assumed and the cases for off-site power being available and unavailable are considered. In the case of the consequential LOOP, the operator is required to open one PSV to get the RCS pressure down to reactor heat removal system (RHRS) injection pressure since the water in the loops of the affected SG and the one SG without an EFWS pump (single failure) are not cooled by mixing since the RCPs are not available. EDF and AREVA argue that the systems required are adequately classified against their safety functional role. I accept these arguments.

203 EDF and AREVA argue that move from controlled state to safe shutdown state for the other decrease in heat removal faults are bounded by the feedline break case. This ignores the fact that these events are more frequent and so there is a need to demonstrate a diverse means of reaching the safe shutdown state. This issue has been raised as Action 9 under the GDA Issue, **GI-UKEPR-FS-02**.

4.2.3.8 Radiological Consequence Assessment

204 SAPs FA.3 and FA.7 require that a radiological consequence assessment should be performed on a conservative basis for each design basis fault sequence that can lead to the release of radioactive material. A detailed review of the radiological consequence assessment methodology applied by EDF and AREVA to design basis faults is presented

in Section 4.3 below. The conclusion of this review is that further substantiation and justification is still required as part of new site specific radiological consequence analyses, but it is my judgement that the current methodology presented in the PCSR (Ref.12) is broadly appropriate for this preliminary Step 4 GDA Assessment of individual faults against Target 4 in the HSE SAPs.

205 The PCSR argues that the inadvertent closure of all MSIVs fault and the loss of normal feedwater flow fault are bounded by the release from loss of condenser vacuum fault, which is a PCC-2 event (together with a single failure that results in the failure to isolate the MSRT) since the steam releases will be equivalent. The releases from the condenser vacuum fault comfortably meet the Target 4 limit. In the case of a feedwater system pipe break, EDF and AREVA argue that the radiological consequences are bounded by the release from a PCC-4 two tube SGTR fault. EDF and AREVA have calculated that this latter event gives an off-site dose to an individual of about 2 mSv. Given that the SGTR fault is assumed to result in the direct leak of primary coolant to atmosphere, it is judged that results from a main feedline fault will be bounded by this fault. Given the expected frequency for a PCC-4 fault, it is judged that the requirements of Target 4 of the SAPs have been met.

4.2.3.9 Findings

206 Following my assessment of the decrease in heat removal faults, I am broadly content with the fundamental design of the UK EPR to protect against this class of fault. It is judged that the sizing of the EFWS pumps, the MSRTs, the MSSVs and the pressuriser on the UK EPR are sufficient to provide adequate protection against these faults. I also welcome the decision by EDF and AREVA to implement a modification on the diverse protection system to trip the reactor on high hot leg pressure and to actuate the EFWS on the very low SG level. Progress with these modifications will be monitored under the GDA Issue on diversity, **GI-UKEPR-FS-02** (Action 1) and the cross-cutting GDA Issue, **GI-UKEPR-CC-02**.

207 Two Assessment Findings have been raised (**AF-UKEPR-FS-09** and **AF-UKEPR-FS-10**) associated with the maintenance arrangements for the EFWS. As neither of these are fundamental issues of design, it is my judgement that they can closed out as part of the site licensing process before fuel is brought onto site.

208 The requirement for the Assessment Findings raised in Section 4.2.2 on MANTA validation (**AF-UKEPR-FS-06**) and for the analysis presented in the PCSR to be updated to reflect the UK EPR design (**AF-UKEPR-FS-08**) is additionally supported by the assessment of decrease in heat removal faults.

4.2.4 Electrical Supply Faults

4.2.4.1 Summary of EDF and AREVA's Safety Case

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

210 EDF and AREVA have already explicitly considered many of these faults within other fault classes. For example, short-term and long-term LOOP are considered in the decrease in heat removal faults discussed in Section 4.2.3 above, while forced reduction in flow faults caused as a result of changes in grid frequency are discussed in Section 4.2.5 below. An exception is the work reported in Chapter 16.1.3.3 of the PCSR (Ref. 12) which presents

RRC-A fault category analysis for a station black-out fault caused by loss of off-site power together with common mode failure of the EDGs.

211 The basis of the EDF and AREVA safety case is that they have provided additional power sources in the form of two SBO diesel generators to bring the plant back to a safe final state. The diesels are manually started from the control room. After starting the diesels, manual actions ensure the start-up of the EFWS pumps in divisions 1 and 4. The operator also opens a header to enable feedwater supply to all four SGs and initiates cooldown of the reactor by opening the MSRT valves to ensure the long-term protection of the RCP seals against thermal and mechanical loads. In this way, the seals remain leak tight and there is no loss of primary coolant and the removal of residual heat is assured.

4.2.4.2 Assessment

212 In their response to RO-UPEPR-40 (Ref. 26), EDF and AREVA have acknowledged that they need to perform a review to see if any electrical system faults identified from future PSA screening analysis are potential candidates for design basis analysis. This has been raised as an action under GDA Issue **GI-UKEPR-FS-05**, covering the design basis analysis of essential support systems to ensure that the requirements of SAPs FA.4 and FA.5 are met. In addition, where any of these electrical faults are frequent faults, EDF and AREVA have been asked to demonstrate functional diversity under the GDA Issue **GI-UKEPR-FS-02** on diversity (Action 8).

213 During GDA Step 4, EDF and AREVA were requested to review all frequent PCC initiating events to demonstrate functional diversity. However, their response to RO-UKEPR-41 does not consider loss of essential support systems such as LOOP with common mode failure of the EDGs. Furthermore, although EDF and AREVA discuss this sequence within the RRC-A analysis, no transient analysis is presented, although it is stated that the SGs will dryout after 1.5 hours without feedwater. Given that the RCPs will be tripped following loss of off-site power (significantly reducing the amount of heat generated within the primary circuit) this time appears sensible. The time scales proportionally with the RRC-A analysis for the total loss of feedwater fault presented, in which the RCP pumps are assumed to remain in operation and the SG dryout occurs after 1.2 hours. EDF and AREVA assumed that the operator needs to start the EDGs after 30 minutes and is able to start-up the two EFWS pumps after 45 minutes. The operator is assumed to open the EFWS header after 1.5 hours and commence cooldown after 2 hours using the MSRTs.

214 Clearly, EDF and AREVA will need to provide transient analysis to confirm these claims in their response to **GI-UKEPR-FS-02**. In addition, given the timescales involved for operator action and the serious consequences should the operator fail to meet the actions, EDF and AREVA have also been asked to look into the feasibility of automating the start-up of the SBO diesels from a diverse reactor protection system.

4.2.4.3 Findings

215 As part of GDA Issue **GI-UKEPR-FS-05**, EDF and AREVA have been requested to review any electrical system faults identified from future PSA screening analysis as potential candidates for design basis analysis. In addition, as part of GDA Issue on diversity, **GI-UKEPR-FS-02**, EDF and AREVA have been requested to demonstrate functional diversity for all frequent loss of essential support system faults (Action 8).

Finally, they have been specifically asked to review the feasibility of automating the actuation of the SBO diesels following LOOP with failure of the RPS to actuate the EDGs.

4.2.5 Decrease in Reactor Coolant System Flow Rate Faults

4.2.5.1 Summary of EDF and AREVA's Safety Case

216 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.

217 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 RCS 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 RPS is able to trip the reactor sufficiently quickly to avoid significant fuel damage.

4.2.5.2 Assessment (Overview)

218 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 (loss of one reactor coolant pump);
- short term loss of off-site power (≤ 2 hours - affecting 4 pumps);
- forced decrease in reactor coolant flow (affecting 4 pumps);
- reactor coolant pump shaft seizure (locked rotor); and
- reactor coolant pump shaft break.

219 The first two are PCC-2 events, the third a PCC-3 event, and the last two are PCC-4 events according to the classification scheme of EDF and AREVA. The short term loss of power (≤ 2 hours) is also included in the decrease in heat removal faults in Section 4.2.3 above. It is listed here since the consequential loss of forced coolant flow makes it one of the more limiting faults in terms of DNB criteria.

220 I have chosen to sample the third fault listed above because it is the most limiting fault to protect against in terms of the DNB criteria. In addition, although EDF and AREVA classify it as 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. However, by classifying the fault as PCC-3, EDF and AREVA's design rules allow DNB and limited fuel rod damage to be conceded. I therefore considered that it merited further scrutiny.

221 EDF and AREVA have considered the PCC-2 short term LOOP in their response to RO-UKEPR-41 to demonstrate the diverse protection of the UK EPR to this type of fault. I have therefore assessed their submission demonstrating the tolerability to a failure of the control rods to insert. However, as I explain below, the frequency of the limiting decrease in reactor coolant flow fault is such that it is a potential candidate for the diversity demonstration.

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

Fault Sequence Analysis

222 The sampled fault is the forced decrease of reactor coolant flow as a result of the simultaneous reduction in speed of all four RCPs due to a perturbation of the grid frequency. The case studied assumes that the grid frequency reduces at 4 Hz a second to 0 Hz where it remains for an undetermined period. Such a fast grid frequency drop leads to a reversal of the motor torque, which reduces the speed of the RCPs more rapidly than the voltage drop associated with LOOP case where the pumps coast down in speed at a rate determined by the inertia of the flywheel. EDF and AREVA treat the fault as a design basis transient which meets the requirements of SAPs FA.4 and FA.5. As multiple redundancy is provided within the RPS, the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met (in the analysis, the RCCA with the greatest worth is assumed to remain out of the core but this will have a small effect).

223 The aim of the analysis presented in Ref. 12 is to demonstrate that the RPS can successfully trip the reactor sufficiently quickly to avoid more than 10% of the fuel going into DNB although, in my opinion, this criterion does not represent the ALARP position as it should be possible to demonstrate for this fault that no fuel undergoes DNB. The fault is a race between the speed of the RCPs slowing down and the speed of the RPS to trip the reactor and the RCCAs to insert. It should be noted that major parameters of this fault analysis, such as RCCA insertion times and RCP coast-down times, can be confirmed during commissioning tests on the reactor prior to operation. There is no discussion about achieving successful post-trip cooling since EDF and AREVA judge that this is bounded by the decrease in heat removal faults discussed in Section 4.2.3 above.

Methods and Assumptions

224 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling this loss of coolant flow fault, EDF and AREVA have made the following assumptions to ensure a robust and conservative assessment:

- a power level to the high core power of 102% is assumed;
- the maximum steady-state average temperature taking into account uncertainty of 2.5°C is assumed;
- the minimum steady-state coolant pressure taking into account uncertainty of 2.5 bara is assumed;
- the nominal thermal-hydraulic flow rate is assumed;
- an initial core axial off-set of 18% is assumed;
- the initial DNBR value is set equal to the low DNBR Limiting Condition of Operation (LCO) value;
- the lowest moderator density coefficient is assumed;
- the maximum Doppler coefficient is assumed;
- the fuel to coolant heat transfer coefficient is minimised;
- the RCCA with the greatest worth is assumed to remain stuck out of the core; and
- a conservative delay of 0.6 seconds is assumed before the RCCA start to drop.

225 Of these assumptions, the most significant are the flow rate, the initial power distribution defined by the axial off-set, the initial DNBR value and the moderator density coefficient. These assumptions are generally consistent with standard design basis approaches for such faults and are comparable to those applied in the Sizewell B analysis. They are judged to result in a bounding assessment meeting the requirements of SAP FA.7.

226 The exceptions are the choice of the axial offset (AO) and the initial power distribution assumption, both of which are very conservative. Instead of making bounding choices for the radial power distribution factor, $F_{\Delta H}$, defined from the fuel management studies, EDF and AREVA treat this parameter as a free variable within the safety analysis which is adjusted in a series of sensitivity studies until the minimum DNBR value during the LOOP transient is equal to 1.0 following reactor trip on low RCP speed. The initial DNBR value at the start of the transient, 1.26, then becomes a limit and condition for safe operation, the $DNBR_{LCO}$ value. The methodology then backs-off this value within the site compliance arrangements by taking into account additional uncertainties including the in-core instrumentation to get a $DNBR_{site}$. The uncertainty quoted in the PCSR (Ref. 12) is 32% although this is currently under review. EDF and AREVA have yet to explain and justify to HSE ND how this value is derived. This gives a minimum $DNBR_{site}$ limit of 1.26 x 1.32 = 1.66. The in-core instrumentation is then used to ensure that the minimum operational steady-state DNBR on the reactor remains compliant with this limit. The justification of this uncertainty allowance has already been raised above in Section 4.2.2 as Assessment Finding **AF-UKEPR-FS-04**.

227 It is worth noting that this methodology is applied to all “type-2” transients. These are transients where DNB is the safety parameter of concern and for which the in-core instrumentation is not able to provide a direct transient trip parameter. Reactor coolant flow reduction faults are the most limiting example and so it is the LOOP transient which defines the LCO limit (compliance being demonstrated by the in-core flux instrumentation). This contrasts with “type-1” transients where DNB is again the safety parameter of concern and for which the in-core flux instrumentation is able to provide a direct transient trip parameter, low DNBR, which the reactor protection calculates in real time. These tend to be reactivity faults such as RCCA bank withdrawal faults at power. Finally, there are “type-3” transients where DNB is the safety parameter of concern and for which the reactor starts at zero power and so the in-core instrumentation is not effective. Steamline break faults from hot zero power conditions are a good example.

228 The EDF and AREVA analysis use the SMART 3D reactor kinetics computer code and the THEMIS thermal hydraulic computer code coupled together to model these forced decrease in reactor coolant flow rate transients. The FLICA sub-channel thermal hydraulic code is used to evaluate the number of rods entering DNB. The validation evidence for the SMART and FLICA codes is assessed against SAPs FA.17 to FA.22 in the Fuel and Core Assessment Report (Ref. 15). The THEMIS code has not been assessed on the basis that the analysis in the PCSR that was performed using the code is gradually being replaced by analysis performed using MANTA which is discussed in Section 4.2.2.8.

Transient Analysis

229 The analysis results for the forced reduction of reactor coolant flow are reported in Chapter 14.4.9 of the PCSR (Ref. 12) with additional information in Section 14B.2.6 of Appendix 14B (also Ref. 12). It is worth contrasting this study with the LOOP case which is reported in Chapter 14.3.6 of the PCSR again with additional information in Section

14B.2.5.1 of Appendix 14B. For the forced reduction case, the results predict that less than 1% of the fuel enters DNB. EDF and AREVA state that this meets their acceptance criteria of less than 10% of the fuel enters DNB for a PCC-3 event.

230 These results are not surprising given that EDF and AREVA have defined the LCO limit for DNB using the LOOP fault as the limiting fault. It follows that if the LCO limit is set so as to just avoid fuel entering DNB for the LOOP case, a slightly more onerous flow reduction transient will inevitably result in some fuel rods entering DNB for a limit period of time of a few seconds. Given that a grid frequency variation in UK should probably be considered a frequent event, it is not clear that accepting limited fuel damage for this fault is an acceptable ALARP position given that a slight change in the LCO limit could eliminate the possibility of any fuel damage. As this is a matter associated with determining the technical specification limits and conditions for the fault rather than a fundamental issue with the UK EPR design, I have raised an Assessment Finding, **AF-UKEPR-FS-11**, requiring a future licensee to review the feasibility of adjusting the LCO limit to avoid departure from DNB for this fault. As part of the action, the licensee will need to consider the effects of the turbine governor valve increasing the initial reactor power in response to a perturbation in the grid frequency.

231 In my judgement, forced reduction of reactor coolant flow due to grid frequency drop should have been considered as the limiting frequent fault in this fault class. However, EDF and AREVA have not explicitly analysed this fault in their response to RO-UKEPR-41 in order to demonstrate functional diversity. Instead, they argue that the LOOP ATWT adequately covers this fault. This is because once the RPS signals reactor trip on low RCP speed, the power to the RCPs is tripped (even though the RCCAs do not insert) and the subsequent flow reduction will then be the same as the loss of off-site power case. Although the initial flow reduction will be quicker, the trip (on RCP speed) will also be quicker and in their judgement the effect on DNB will be insignificant. Given the discussion of these faults above, I accept their argument recognising that the more realistic assumptions for axial off-set and $F_{\Delta H}$ that are applied in ATWT analysis should ensure that the fuel failure criterion is met. However, I believe that this should be confirmed during site licensing under Assessment Finding, **AF-UKEPR-FS-12**.

232 In their response to RO-UKEPR-41 (Refs 45 and 46) EDF and AREVA have identified the need to analyse the following fault sequences:

- short-term loss of off-site power with failure of the control rods to insert following reactor trip; and
- short-term loss of off-site power with failure of the RPS to initiate a reactor trip signal.

The transient analysis in support of these fault sequences is discussed below.

Loss of Off-Site Power with Failure of the RCCAs to Insert

233 In the case of LOOP with failure of the RCCAs to insert, the risk reduction feature that has been introduced to provide protection is an ATWT signal that is triggered by the RPS 20 seconds after a reactor trip signal if either three RCCAs or more are not inserted to the bottom of the core or there is a high flux signal. The ATWT signal automatically initiates the EBS and isolates the CVCS. This strategy differs from that applied at Sizewell B, which is provided with a diverse emergency boration system to protect against ATWT faults. EDF and AREVA are claiming that the combined effects of the automatic actuation of the EBS, the tripping of the turbine and the initiating event tripping, the RCPs

will provide adequate protection for such faults, given the inherent characteristics of PWR moderator temperature coefficients.

234 The analysis reported in their RO-UKEPR-41 response (Ref. 46) is performed on a conservative basis consistent with design basis assumptions and so BOC conditions are chosen with the moderator temperature coefficient set at -13.2 pcm/°C. The core power is assumed to be at 102% and the thermal hydraulic design flow rate is chosen. The flow capacities of the PSVs are penalised as are the trip setpoints and signal time delays. 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. The analysis is performed with the MANTA, SMART, and FLICA III coupled code analysis route discussed in Section 4.2.2.

235 The results presented (Ref. 46) show that at five seconds the LOOP signal trips the turbine, the RCP pumps and the main feedwater pumps. As the levels in the SGs decrease due to the loss of main feedwater, the pressure and temperature of the RCS start to increase. After seven seconds a reactor trip signal is generated on low RCP speed when the speed passes below the 91% setpoint but the RCCAs are assumed to fail to insert. The pressure continues to increase until two of the PSVs open at 14 and 16 seconds respectively. The ATWS signal is generated 20 seconds after the reactor trip signal actuating the EBS. The tripping of the RCP pumps causes an increase in the voiding of the core resulting in a rapid reduction in core power. The PSVs re-close. The EFWS is also actuated at 470 seconds on low SG level. After 500 seconds the boron injected from the EBS enters the core and the reactor starts to shutdown. Although the primary system goes water solid, the flow capacity from just one of the three PSVs valves is sufficient to keep the pressuriser pressure below 176 bara. The peak pressure in the primary circuit will be slightly higher but still significantly less than the structural integrity limit of 228 bara. The reduction in power caused by the RCPs coasting down, together with rise in pressure, is sufficient to ensure adequate margin to DNB. The minimum DNB of 2.12 occurs seven seconds after pump trip. This is only slightly lower than the initial value of 2.17 and well above the safety limit of 1.21.

236 The analysis for this fault, like that for the excessive increase in secondary side flow and the inadvertent operation of the pressuriser spray cases, assumes that all the control rods fail to enter the core. It does not consider the possibility of mechanical failure causing only partial RCCA insertion. In such circumstances, there is the potential for insufficient RCCAs to insert to fully shutdown the reactor and for the flux power distribution to become distorted with small regions of the core remaining critical due to the failure of the RCCAs to insert. For this reason, I am requesting any future licensee to perform such analysis under Assessment Finding **AF-UKEPR-FS-13** to see if it places any constraints on the fuel management scheme for the reactor core. However, my judgement is that it is unlikely to result in any changes to the reactor design. This judgement is further supported by some confirmatory analysis performed by GRS which is reported below.

237 In addition to the analysis performed in response to RO-UKEPR-41, EDF and AREVA have also calculated this transient within the RRC-A sequence analysis reported in Chapter 16.1 of the PCSR (Ref. 12) using a best estimate analysis for the 4250 MWth reactor design. The analysis confirms that although the reactor goes water solid, the flow capacity from a single PSV (analysed using the previous SEBIM design of valve rather than the latest SEMPELL valve) is sufficient to keep the pressuriser pressure below about 177 bara and the primary pressure below about 185 bara while the minimum DNBR is 2.36 which is comfortably above the 1.21 criterion. This case is reported because it has been used as a benchmark case for some confirmatory analysis performed by GRS.

Confirmatory Analysis

238 GRS has repeated the RRC-A loss of off-site power ATWT case using its own ATHLET systems code and its 3D QUABOX/CUBBOX reactor kinetics code coupled together as well as a point kinetics comparison. The results of GRS comparison (Ref. 49) show good agreement with EDF and AREVA's predictions, recognising that the GRS calculations assume a different moderator temperature coefficient due to a lower initial boron concentration which will ensure a more negative temperature coefficient. The expected pressure rise for the GRS results should therefore be slower than the EDF and AREVA's predictions since the reactor power will fall quicker for a given temperature rise. The GRS analysis also models the latest SEMPELL valves.

239 The secondary side predictions are very similar. Primary side temperatures are also in good agreement. The GRS power level falls off quicker as expected. The main difference is in the pressure response and the flow through the PSVs. However, I have compared the GRS predictions with the RO-UKEPR-41 predictions (Ref. 46) for this sequence (which also models the latest SEMPELL valves and the timings). The shape of the pressure response predicted by GRS is almost identical to the EDF and AREVA's more recent analysis. The comparison of predicted power transient and reactivity changes are also very good.

240 The initial vapour flows through the PSVs are very similar. The GRS 3D coupled code calculation does not predict a second lifting of the 1st PSV but the GRS point kinetics calculation does predict a second lift and at almost the same time. However, the GRS predicted liquid flow transient though the 1st PSV is 300% greater. Nevertheless, given that the results are effectively blind comparisons, since neither EDF and AREVA nor GRS have seen each others results, I judge the agreement to be excellent.

241 The GRS prediction of DNB uses two different critical heat flux correlations and so comparisons with the EDF and AREVA analysis are complicated. However, the general trend of the GRS point kinetics calculations agrees reasonably well with the EDF and AREVA predictions, although it does predict a greater fall during the initial phases of the transient. Nevertheless, significant margins to DNB are predicted by GRS.

242 GRS has performed a number of sensitivity studies for the case of partial RCCA insertion discussed above. In particular, it has studied eight RCCAs inserted in one quadrant of the core and twelve RCCAs inserting around the perimeter of the core. The effect is only marginal on the minimum DNBR and indeed in the case of the eight asymmetric RCCAs the DNBR margin increases.

243 As in the case of the loss of main feedwater with failure of the RCCAs to insert (Section 4.2.3), the comparisons have increased my confidence in the EDF and AREVA analysis. In my judgement, there is no justification for requiring EDF and AREVA to install a fast acting emergency boration system on the EPR on the basis of these results. It is worth noting that the fast acting emergency boration system on Sizewell B is in any case 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. In my judgement, the results presented by EDF and AREVA suggest that adequate protection is already provided for this fault sequence and that the requirements of SAP FA.7 and RO-UKEPR-64 (through the response to RO-UKER-41) have been met without the need for further protection.

244 Finally, it is worth contrasting the minimum DNBR values quoted in the best estimate analysis performed by EDF and AREVA in their RRC-A analysis, the best estimate

analysis performed by GRS in its confirmatory analysis, the more conservative analysis performed by EDF and AREVA in their response to RO-UKEPR-41 and the conservative design basis analysis performed by EDF and AREVA as presented in the PCC section of the PCSR (just before the point of reactor trip) since all these analyses have been performed using 3D coupled code analysis of the same loss of off-site power fault. The PCC analysis shows a significant change between the initial $DNBR_{LCO}$ limit and the minimum DNBR value (1.24 to 1.00) over about the first 2.5 seconds up until when the reactor trips. The other studies show only very slight reductions over first 10 seconds or so until the core power significantly reduces following the turbine trip when the minimum DNBR increases significantly. For example, for the RO-UKEPR-41 analysis, the minimum occurs at 6 seconds (2.17 to 2.12). The minimum for RRC-A analysis is 2.36. Given the similarity of the RRC-A analysis and the RO-UKEPR-41 response it is clear that many of the "conservative" assumptions (initial power level, thermal design flow rate) in the RO response have very limited effects on the minimum DNBR value. Since, in the case of EDF and AREVA analyses, even the same models are being used, it is clear that the differences between the results of the PCC study and the other ATWT studies is wholly associated with the initial power distribution assumed in terms of the AO of 18% and the $F_{\Delta H}$. None of these values are quoted for the ATWT studies but it is stated that they come from bounding values for the reference core fuel management studies. In contrast, the LCO value for AO on Sizewell B is 3%. The design basis calculation therefore assumes an axial power distribution that will peak higher up in the core and will also have a greater absolute value. The design basis calculations have been performed on a very conservative basis which will penalise the DNBR prediction with an AO value that corresponds to the axial off-set trip point.

245 However, this raises the question of whether the AO assumed in the ATWT analysis reported in the RO response (Ref. 46) is adequately conservative. Even for the fault sequences associated with an ATWT event, HSE ND would expect a calculation supporting safety analysis to be performed at a 95% confidence level for any key input parameter. For a loss of grid fault, it is likely that there could have been some grid frequency perturbations before the event that causes the loss of off-site power. Such perturbations are likely to result in the movement of control rods within the core, such that it is not clear whether it is appropriate to assume the unperturbed reference fuel cycle AO as the input parameter for these calculations. In addition, the grid frequency perturbations can potentially cause the turbine governor valve to increase the initial reactor power. In the UK, ATWT sequences are considered within the design basis. In my judgement, there is a need for any future operator to justify the choice of AO value that is assumed in such calculations when used to derive the $DNBR_{LCO}$ limit for the technical specifications. I have therefore raised an Assessment Finding, **AF-UKEPR-FS-14**, requesting that such studies be performed in support of the derivation of the technical specification limits and conditions during the site licensing process.

Loss of Off-site Power with Failure of RPS to Initiate a Reactor Trip Signal

246 As part of CMF#23 (Ref. 42), EDF and AREVA are proposing a new trip signal to be provided on a diverse protection system to trip the reactor on low RCP speed when the speed reduces to 91%. This is principally for the case of the RPS failing to trip the reactor following forced reduction in flow fault (for which EDF and AREVA did not perform analysis in Ref. 46). However, it will also be beneficial for the case of the RPS failing to trip the reactor following a LOOP. In the current design (Ref. 12), the PAS is claimed to trip the reactor and turbine following receipt of a low 3 SG level signal due to the loss of

main feedwater associated with the loss of off-site power. The design change will reduce the time until the reactor trip occurs which is a positive development from a safety perspective and is fully supported. Its implementation will be monitored under Action 3 of GDA Issue **GI-UKEPR-FS-02**.

247 The analysis reported in their RO-UKEPR-41 response (Ref. 46) does not claim this new trip signal. Instead, a trip on high hot leg pressure is claimed (which is also one of the extra trip parameters that are being introduced under CMF#23). The calculation is performed on a conservative basis consistent with design basis assumptions and so BOC conditions are chosen with the moderator temperature coefficient set at -13.2 pcm/°C. The core power is assumed to be at 102% and the thermal hydraulic design flow rate is chosen. The flow capacities of the PSVs are penalised as are the trip setpoints and signal time delays. With the RPS unavailable, the MSRTs cannot operate and so the MSSVs are claimed instead. 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. The analysis is performed with the MANTA, SMART, and FLICA III coupled code analysis route discussed in Section 4.2.8 up until the time of trip. Following reactor trip, the MANTA code is used in standalone mode with its point kinetic model.

248 The results presented (Ref. 46) show that as the SGs empty due to the loss of feedwater, the pressure and temperature in the RCS start to increase. Unlike the previous case where a mechanical failure prevents the control rods inserting, no reactor trip signal is generated on high pressuriser pressure due to assumed failure of the RPS. Instead, the reactor trip signal is generated by the proposed new high hot leg pressure trip signal on the diverse reactor protection system after 13.7 seconds. The pressure continues to increase until one of the PSVs opens at 14 seconds. It re-closes at 31.5 seconds. Despite the primary system going water solid, the flow capacity from just one of the three PSVs valves is sufficient to keep the pressuriser pressure below 176 bara. Although the peak pressure in the primary circuit will be about 10 bar higher, this is still well below the structural integrity limit of 228 bara. As in the previous case, the rise in pressure is sufficient to ensure adequate margin is maintained to DNB. The minimum DNBR of 2.12 is reached after 7 seconds, leaving significant margin to the safety limit of 1.21. However, a significant difference to the previous sequence is that the EFWS is not actuated because the RPS is unavailable. EDF and AREVA argue that after 30 minutes the operator can start the EFWS pumps. In practice, the modification to automatically start the EFWS pumps on low SG level identified in the loss of main feedwater ATWT case with failure of RPS under CMF#14 (Ref. 42) will also provide protection for this fault as well. Given the proposed modifications, it is my judgement that the intended protection provided for this fault sequence is adequate to meet the requirements of SAP FA.7.

4.2.5.4 Controlled State to Safe Shutdown State

249 EDF and AREVA argue that the move from controlled state to safe shutdown state for reduction in flow faults is bounded by the feedwater system line break case. While it is accepted that the feedwater system line break transient is more limiting in terms of heat removal requirements, this ignores the fact that decrease in flow events are more frequent and so there is a need to demonstrate a diverse means of reaching the safe shutdown state. This issue has been raised as Action 9 under the GDA Issue, **GI-UKEPR-FS-02**.

4.2.5.5 Radiological Consequence Assessment

250 SAPs FA.3 and FA.7 require that a radiological consequence assessment should be performed on a conservative basis for each design basis fault sequence that can lead to the release of radioactive material. A detailed review of the radiological consequence assessment methodology applied by EDF and AREVA to design basis faults is presented in Section 4.3 below. The conclusion of this review is that further substantiation and justification is still required as part of new site specific radiological consequence analyses, but it is my judgement that the current methodology presented in the PCSR (Ref.12) is broadly appropriate for this preliminary Step 4 GDA Assessment of individual faults against Target 4 in the HSE SAPs.

251 The PCSR argues that these loss of flow faults are bounded by the release from the PCC-2 loss of condenser vacuum fault with a single failure that results in the failure to isolate the MSRT since the steam releases will be almost equivalent. The releases from the condenser vacuum fault comfortably meet the Target 4 limit.

4.2.5.6 Findings

252 Following my assessment of the decrease in reactor coolant flow faults, I am broadly content with the fundamental design of the UK EPR to protect against this class of fault. It is judged that the sizing of the inertia of the RCP flywheels and the low RCP speed setpoint protection are sufficient to provide adequate protection against these faults.

253 I welcome the decision by EDF and AREVA to implement a modification to provide a low RCP speed reactor trip signal on the diverse protection system. This modification is a significant safety improvement and, in my judgement, complements the proposals to implement high hot leg pressure trip signal and to actuate the EFWS on the very low SG level already discussed under the loss of main feedwater fault in Section 4.2.3.5). Progress with these modifications will be monitored under the GDA Issue on diversity, **GI-UKEPR-FS-02** (Action 3) as well as under the cross-cutting GDA Issue **GI-UKEPR-CC-02**. Importantly, I do not consider that there is a need to implement a fast acting emergency boration system on the UK EPR, such as that which has been provided for Sizewell B, as I do not believe it will contribute significantly to the improvement of safety on the plant.

254 Four Assessment Findings have been raised (**AF-UKEPR-FS-11** to **AF-UKEPR-FS-14**). **AF-UKEPR-FS-11** and **AF-UKEPR-FS-14** are items which require further analysis to define LCO limits. Although they are not expected to be fundamental design issues, in my judgement they should be completed before the affected safety SSCs are delivered to site. Assessment Findings **AF-UKEPR-FS-12** and **AF-UKEPR-FS-13** require additional transient analysis to be performed to confirm that the currently presented analysis is limiting. These two Assessment Findings can be closed out as part of site licensing before fuel is brought onto the site.

255 The Assessment Finding identified in Section 4.2.2 to provide a methodology for determining the DNB uncertainty allowance for Type I and Type II fault transients (**AF-UKEPR-FS-04**) is also a requirement of the assessment of decrease in reactor coolant flow faults.

4.2.6 Reactivity and Power Distribution Anomalies

4.2.6.1 Summary of EDF and AREVA's Safety Case

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

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

258 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.

4.2.6.2 Assessment (Overview)

259 EDF and AREVA have considered the following faults within this category that they consider 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;
- CVCS malfunction that results in a decrease in boron concentration in the reactor coolant;
- uncontrolled single RCCA withdrawal;
- inadvertent loading and operation of a fuel assembly in an improper position; and
- a spectrum of RCCA ejection faults.

260 The majority of the faults listed above are PCC-2 events. The exceptions are inadvertent loading and uncontrolled single RCCA withdrawal faults which are PCC-3 events, and the RCCA ejection fault which is a PCC-4 event.

261 In my GDA Step 3 Assessment Report, I chose to sample three of the above faults types. The first fault considered was 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 PCI failures. The second fault was RCCA misalignment 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 was the RCCA ejection fault, which EDF and AREVA judge to be the most bounding fault in terms of fuel damage. During GDA Step 4, I have extended

my assessment to cover the CVCS malfunction leading to a decrease in boron concentration fault and the inadvertent loading of fuel in an improper position fault.

262 In my GDA Step 3 Assessment Report, I noted that 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. 50) in France. An assessment of this fault has been performed in GDA Step 4 but it is reported in the Fuel and Core Assessment Report (Ref. 15)

4.2.6.3 Assessment of Uncontrolled Withdrawal of an RCCA Bank at Power (Limiting Frequent Fault)

Fault Sequence Analysis

263 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 SAPs FA.4 and FA.5. EDF and AREVA claim that there are multiple redundancies within the RPS 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.

264 EDF and AREVA claim that the following protection channels 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; and
- reactor trip on high pressuriser level.

265 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 also 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.

266 In my GDA Step 3 Assessment Report, I noted that Sizewell B has both a Primary Protection System (PPS) and Secondary Protection System (SPS) through which the following trip parameters are claimed: high cold leg temperature, high positive flux rate (PPS), high positive flux rate (SPS), high flux (PPS) and high N-16 (PPS). I also noted that Sizewell B is provided with diverse flux protection signals on both the PPS and SPS. The DNBR core limit trip, which is roughly equivalent to the low DNBR trip on the UK EPR (although the Sizewell B trip signal is based upon the N-16 detectors rather than the in-core detectors for the UK EPR), 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. 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. Instead, it possesses in-core detectors which are connected to the protection

system and so can trip the reactor automatically. In my GDA Step 3 Assessment Report, I stated that in my judgement, the provision of in-core detectors connected directly to the RPS on the UK EPR represents a significant safety improvement over the ex-core detectors that were provided on earlier PWR designs, and that in principle, there appeared to be diversity to the ex-core detectors on the UK EPR, meeting the requirements of SAP ESS.7. I noted, however, that the intent was that both systems would only be connected to the same digital RPS. Under modification CMF#23 (Ref. 42), EDF and AREVA are now proposing to add a high flux trip signal to the diverse reactor protection system. They are also adding a high axial offset trip and a high hot leg pressure trip signal on to the diverse protection system under the same modification. In my judgement, these proposals represent a significant safety improvement and are fully supported. The implementation of these modifications will be monitored under GDA Issue, **GI-UKEPR-FS-02** (Action 4).

267 In my GDA Step 3 Assessment Report, I noted that there was no discussion of PCI failures as a result of the reactivity insertion faults within the EDF and AREVA analysis. During GDA Step 4, in response to RO-UKEPR-42, EDF and AREVA have performed analysis to demonstrate that for faults more frequent than 1 x 10^{-3} per year the RCSL system is able to provide sufficient protection to prevent fuel failures due to PCI. This work has been assessed, but is reported in the Fuel and Core Assessment Report (Ref. 15).

Methods and Assumptions

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

- Power levels at 10% and 102% are analysed (for the 4900 MWth EPR design).
- The radial peaking factor $F_{\Delta H}$ has a value of 1.85 adjusted so that the initial DNBR value is set equal to the DNBR LCO value for the full power case and is kept constant during the transient.
- A bounding range of reactivity insertion rates from 0 to 90 pcm/s are assumed.
- Studies are performed assuming both the maximum and minimum moderator density coefficient.
- When the minimum moderator density coefficient is assumed, its value is taken to be zero and the minimum Doppler coefficient and kinetic coefficients are assumed.
- When the maximum moderator density coefficient is assumed, the maximum Doppler coefficient and kinetic coefficients are assumed.
- The fuel to coolant heat transfer coefficient is maximised.
- The RCCA with the greatest worth is assumed to remain stuck out of the core.
- The setpoint values include instrumentation and setpoint uncertainties and the maximum time delays are assumed within the analysis.

269 The EDF and AREVA analyses use the THEMIS and FLICA computer codes to model these uncontrolled RCCA bank withdrawal faults. The assessment of the FLICA code against the validity of assurance SAPs FA.18 to FA.22 is reported in the Fuel and Core

Assessment Report (Ref. 15). As noted previously, the THEMIS thermal hydraulic code is gradually being replaced by the MANTA code and so it has not been assessed during Step 4. The THEMIS code uses a point kinetics model.

270 These methods and assumptions represent a standard approach to the design basis analysis of such faults and are comparable to those applied in the Sizewell B analysis, with the exception of the approach to determining $F_{\Delta H}$ although it is judged to represent a bounding value. Taken together, these assumptions are judged to result in a bounding assessment meeting the requirements of SAP FA.7.

Transient Analysis

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

272 The analysis results of EDF and AREVA are summarised in Figure 14 of Chapter 14B.2.10 of the PCSR's Appendix 14B (Ref. 12) which presents the minimum DNBR as a function of reactivity insertion rate for the minimum reactivity feedback coefficient for the 100% power case. 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.

273 When the same minimum feedback cases were analysed for Sizewell B, results were presented for 100% and 80% power operation because sensitivity studies demonstrated that the 80% power case is the most bounding in terms of DNB. All the trip parameters that are claimed were presented (Ref. 39). Sizewell B also takes account of the possible effects of grid frequency perturbations on the initial conditions of the fault. In contrast, the only reactor trip parameters plotted by EDF and AREVA on Figure 14 are the high flux rate of change and low DNBR trips. Since no other reactor trip parameters are presented it has not been possible to verify whether these signals are functionally capable of protecting against the fault when assessed against the requirements of SAPs ESS.2, ESS.4 and ESS.6. In my judgement it is unlikely that any of these reactor trip signals will be able to provide effective protection against DNB over the whole range of reactivity insertions speeds that is being considered. The figure shows that even the trip parameters that are plotted do not provide effective protection over the full range of reactivity insertion speeds. For example, the trip on low DNBR is seen to be ineffective at faster insertions speeds. In contrast, the Sizewell B analysis plots all the trip parameters over the full range of insertion speeds and demonstrates that there are always two trip parameters that provide effective protection against DNB for the full range of reactivity insertion speeds.

274 In my view, there is a need to demonstrate that diversity of protection against DNB exists for the full range of fault speeds and power levels. I have therefore raised Assessment Finding **AF-UKEPR-FS-15**. However, I recognise that additional protection has already been proposed and that assumptions made in the fault analysis initial radial power profile and axial off-set distribution are conservative. As a result, it is my judgement that the requisite additional analyses are unlikely to require any further plant modifications, recognising that there is scope for reducing the conservatism in the assessment as the sequence frequency reduces.

275 EDF and AREVA have, in-effect, already demonstrated that some aspects of UK EPR design can tolerate common mode failures in the form of ATWT analysis performed within the RRC-A analysis. This has been supplemented by work performed under RO-UKEPR-41 (Ref. 10). In their response (Refs 45 and 46), they have identified the need to consider the following fault sequences:

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

276 EDF and AREVA argue that the uncontrolled RCCA bank withdrawal with subsequent failure of the RCCAs to insert fault sequence (for some mechanical reason) is bounded by the uncontrolled RCCA bank withdrawal with failure of RPS to trip the reactor. This is because a functioning RPS will still freeze further movements of the withdrawing bank despite the RCCAs being unable to insert. Hence, they have not explicitly analysed the transient. I accept this argument.

277 The case of the RPS failing to trip the reactor following an uncontrolled RCCA withdrawal will be amongst those faults benefitting from the introduction of three new trip signals (high flux, high axial offset and high hot leg pressure low) proposed under modification CMF#23 (Ref. 42). Previously, in the RRC-A analysis, the PAS was claimed to trip the reactor and turbine following receipt of a low 3 SG level signal due to the loss of main feedwater associated with the loss of off-site power. This will reduce the time until the reactor trip occurs which is a positive development from a safety perspective and is fully supported.

278 The analysis reported in their RO-UKEPR-41 response (Ref. 46) for the uncontrolled RCCA withdrawal with failure of RPS to initiate a reactor trip signal did not meet my expectations. The calculation is performed on a very conservative basis consistent with design basis assumptions made in the PCC-2 analysis of EDF and AREVA for this initiating fault. Very bounding assumptions are made about the initial power distribution. The initial axial offset is set at 12% which is just below the axial offset trip setpoint. This results in an axial profile that is peaked in the top half of the core. The radial power factor, $F_{\Delta H}$, is set equal to 1.91 to minimise the initial DNBR value. The maximum RCCA withdrawal rate of 75 step/min is assumed. At the time of trip, the hot channel heat flux hot rod factor, F_q, has increased from 2.88 to 3.0 and the axial offset has increased to 30%. The analysis is performed with the MANTA, SMART, and FLICA III coupled code analysis route discussed in Section 4.2.2. However, all these conservatisms have resulted in almost 9.2% of the fuel exceeding DNB, fuel melting at the hot spot reaching 5.6% by volume, and the maximum clad temperature reaching 1206°C. EDF and AREVA argue that this meets their PCC-3/4 acceptance criteria. While I accept that it does meet these acceptance criteria, my judgement is that it does not represent an acceptable ALARP position. For these faults, I judge that more appropriate analysis, performed with prudent conservatisms, consistent with a 95% confidence level, would not lead to DNB. Such an analysis is required in support of the determination of the trip setpoints for the proposed new trip signals of high axial offset and high neutron flux on the diverse protection system. As noted in the loss of coolant flow fault due to the loss of off-site power above, there is also a need for any future operator to justify the choice of AO value that is to be assumed in calculations that are being used to derive the $DNBR_{LCO}$ limit for the technical specifications. This need also extends to this fault as such grid oscillations could be the part of the reason for this initiating event to occur. For this reason, Assessment Finding **AF-UKEPR-FS-16**, has been raised for a future licensee to

demonstrate that the setpoints of the new trip parameters on the SAS system are sufficient to prevent the fuel from entering DNB.

279 EDF and AREVA have also calculated this transient within the RRC-A sequence analysis reported in Chapter 16.1 of the PCSR (Ref. 12). Although the analysis is intended to be best estimate, a conservatively high rod RCCA bank withdrawal speed of 75 pcm/min is assumed. The moderator temperature coefficient is -10 pcm/°C and the Doppler coefficient is -2.5 pcm/°C. These values will conservatively cover most fuel cycles. Finally, the $F_{\Delta H}$ is calculated for the reference fuel cycle but assuming the moderator and Doppler coefficients are set at their minimum values which will maximise the value of $F_{\Delta H}$ and result in a conservative assessment of DNBR providing there are no grid perturbations associated with the initiating event. The analysis confirms that the flow capacity from a single PSV (analysed using the previous SEBIM design of valve rather than the latest SEMPELL valve) is sufficient to keep the primary pressure below 181.1 bara while the minimum DNBR is 2.25. The latter is comfortably above the 1.21 criterion. In my judgement, it is likely that the intended protection that EDF and AREVA are providing for this fault sequence will meet the requirements of SAP FA.7. However, the implementation of these modifications will need to be monitored under GDA Issue, **GI-UKEPR-FS-02** (Action 4).

4.2.6.4 Assessment of RCCA Misalignment Faults (Limiting Frequent Fault)

Fault Sequence Analysis

280 RCCA misalignment covers a range of faults from statically misaligned RCCA up to one or more dropped RCCAs within the same group. These are all PCC-2 events. EDF and AREVA argue that for these faults the low DNBR trip using the in-core detectors is very effective so that DNB is avoided. In my judgement, the provision of in-core detectors on the UK EPR that are connected directly to the RPS potentially represents a significant safety improvement over the ex-core detectors that were provided on earlier PWR designs such as Sizewell B. Nevertheless, EDF and AREVA have not provided a justification of the algorithm used by the RPS to determine the low DNBR trip setpoint from the measurements made by the in-core detectors. In particular, no justification has been provided for the uncertainty allowance needed to cover the uncertainties associated with calibration. For this reason, this additional information will need to be supplied as part of the response to Assessment Finding **AF-UKEPR-FS-04** identified in Section 4.2.2 above. In addition, it must also be recognised that these faults are potentially very frequent faults and so 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 PPS for Sizewell B is provided 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. As a frequent fault, I was expecting that the response to RO-UKEPR-41 would include a consideration of such faults with failure of either the RPS or the in-core detection system to trip the reactor. EDF and AREVA have not considered this fault sequence. For this reason, I have asked EDF and AREVA to perform this analysis under GDA Issue, **GI-UKEPR-FS-02** (Action 5).

Confirmatory Analysis

281 GRS has performed (Ref. 51) an independent assessment of the RCCA drop fault using the coupled ATHLET and 3D QUABOX/CUBBOX system and reactor kinetics codes. Its analysis was not able to represent the reactor control system and so the other RCCAs

were not assumed to be withdrawn in response to the dropped RCCA(s) fault. Instead, it is assumed that as an effect of the resultant cooldown caused by the dropped RCCA(s), the moderator temperature coefficient restores the reactor back to normal full power. The transient was in fact modelled as a series of pseudo steady-states to ease the numerical simulation. Studies were done for a single RCCA, a single symmetrical bank of four RCCAs, two cases looking at four asymmetrical RCCAs in one half of the core and one quadrant of the core, and two cases looking at eight asymmetrical RCCAs in one half of the core and one quadrant of the core. The results (Ref. 51) suggest that the asymmetrical RCCA drop cases do result in reductions in the minimum DNBR. For a single RCCA, the DNBR reduction is from 2.78 to 2.61. For eight RCCAs dropping in one half of the core, the change in the minimum DNBR goes from 2.78 to 2.10. While this is still above the DNBR safety criteria, it represents a significant swing, recognising that the analysis has been performed on a best estimate basis. In particular, it ignores the effects of the control system and the short-term xenon transient, both of which are likely to further exacerbate the effect. Given that the UK EPR design is now going to have a new flux signal on the diverse protection system, the feasibility of adding a negative flux trip needs to be considered. This has been raised as Action 5 under GDA Issue, **GI-UKEPR-FS-02**.

4.2.6.5 Assessment of CVCS Malfunction Resulting in a Decrease in Boron Concentration

Fault Sequence Analysis

282 This section of the report considers homogeneous boron dilution faults caused by a failure of the CVCS. Such faults can occur both while the reactor is at power and while it is shutdown. They result in the uniform reduction of the boron concentration in the core and are classified PCC-2 events. It should be noted that heterogeneous boron dilution events, which result in slugs of unborated water being transported into the core, are considered separately in Section 4.14 below.

283 Since uncontrolled boron dilution faults are classified as PCC-2 events, EDF and AREVA treat them as design basis faults meeting the requirement of SAPs FA.4 and FA.5. EDF and AREVA argue that there are multiple redundancies within the protection system and so the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 are automatically met. The transient analysis for the reactor at power event focuses on demonstrating that the protection system can successfully trip the reactor to avoid the fuel going into DNB; on a shutdown reactor the aim is to demonstrate that the reactor remains sub-critical.

284 EDF and AREVA claim the same protection systems as the uncontrolled RCCA withdrawal fault for boron dilution faults occurring at power but with an additional anti-dilution protection channel that monitors boron concentration in the CVCS charging line. In the case of shutdown faults, the following protection systems are available depending on the status of the reactor to protect against this fault:

- anti-dilution in shutdown conditions with RCPs not in operation; and
- anti-dilution in shutdown conditions with RCCAs inserted.

285 EDF and AREVA claim that the anti-dilution protection channels monitor boron concentration in the CVCS charging line using a boron meter.

Methods and Assumptions

286 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling uncontrolled boron dilution faults, EDF and AREVA have made the following assumptions to ensure a robust and conservative assessment for the at power cases:

287 They make the following assumptions with regard to the anti-dilution channels:

- a conservative low estimate for the volume of borated water in the primary circuit is assumed;
- the response delay of the channel is 66 seconds;
- isolation is completed in 40 seconds;
- the maximum make-up flow of 26 kg/s is assumed; and
- the CVCS piping volume is 1.0 m^3.

288 The SMART computer code is used to calculate the critical boron contribution for uncontrolled boron dilution faults occurring at shutdown conditions. The assessment of the SMART code against the validity of assurance SAPs FA.18 to FA.22 is reported in the Fuel and Core Assessment Report (Ref. 34). This analysis effectively determines the moderator temperature coefficient for cold shutdown conditions. These will need to be included within the limits and conditions of the Technical Specifications to ensure future core reload fuel management schemes are compliant with the assumptions.

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

Transient Analysis

290 The PCSR (Ref. 12) argues that boron dilution faults occurring at power are bounded by the uncontrolled RCCA bank withdrawal fault transient analysis discussed above. For shutdown faults, it argues that the anti-dilution channels provide protection against the fault and so transient analysis is provided. This ignores the fact that the fault is classified a PCC-2 event and so under the requirements of RO-UKEPR-41 (Ref. 10) it is a frequent fault for which a demonstration of diversity is required.

291 In their response to RO-UKEPR-41 (Refs 45 and 46), EDF and AREVA have identified the need to assess the following fault sequences:

- CVCS malfunction resulting in boron dilution at power with failure of the RCCAs to insert following a reactor trip signal; and
- CVCS malfunction resulting in boron dilution at power with failure of the RPS to initiate a reactor trip signal.

292 In Ref. 46 EDF and AREVA argue that the CVCS malfunction resulting in boron dilution with failure of the RCCAs to insert fault sequence is bounded by the uncontrolled RCCA bank withdrawal with subsequent failure of RCCAs to insert. This is because the fault is a very slow transient with a reactivity insertion rate of only 2 pcm/s. I accept this argument.

293 EDF and AREVA argue that the CVCS malfunction resulting in boron dilution with failure of the RPS to trip the reactor is bounded by the uncontrolled RCCA bank withdrawal with

failure of the RPS. The basis of their argument is that the fault is a very slow transient with a reactivity insertion rate of only 2 pcm/s. However, EDF and AREVA appear to be considering the failure of the TXS system causing the failure of the RPS and the RCSL. If only the RPS fails then a boron dilution fault will result in the control rods inserting deeply into the core. However, EDF and AREVA have considered this fault in the RRC-A analysis using the SMART, MANTA and FLICA coupled codes. Their analysis shows that this fault results in a more onerous minimum DNBR than the RCCA bank withdrawal case at 2.03 compared with the 1.21 criteria. For this reason there is a need to demonstrate that the new protection proposed under CMF#23 adequately protects against this fault. As a result, I have raised Assessment Finding **AF-UKEPR-FS-17**.

294 It is my judgement that a CVCS malfunction resulting in boron dilution during shutdown with failure of the RPS to initiate anti-dilution protection also needs to be considered. EDF and AREVA have not presented an analysis for this sequence and so it has been raised as Action 7 under GDA Issue **GI-UKEPR-FS-02**.

Confirmatory Analysis

295 GRS has performed an independent assessment of the boron dilution fault at shutdown with failure of the RPS using the coupled ATHLET and 3D QUABOX/CUBBOX system and reactor kinetics codes. The results (Ref. 51) suggest that there are very long time scales for this fault but the analysis uses best estimate moderator temperature coefficients that probably could not be justified for a design basis fault assessment. For this reason, there is still a need for EDF and AREVA to provide a safety case to demonstrate how this fault is protected against, as noted in the previous paragraph under Action 7 of **GI-UKEPR-FS-02**.

4.2.6.6 Assessment of Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position

296 Although this PCC-3 event is discussed in Chapter 14.4.8 of the PCSR (Ref. 12), no explicit analysis is provided for this fault with the reactor at power. Instead, EDF and AREVA argue that the administrative controls and reactor physics test before and during power raise will enable the detection of the fault. Traditionally, a consequence analysis is performed to confirm for the proposed fuel management scheme that following the most onerous inadvertent misloading of two fuel assemblies no fuel will enter DNB upon return to power. It is realised that this is not a fundamental issue with the design of the UK EPR but more an operational safety issue and so an Assessment Finding, **AF-UKEPR-FS-18**, has been raised requiring any future licensee to provide such an assessment during the site licensing process.

4.2.6.7 Assessment of Spectrum of RCCA Ejection Faults (Limiting Infrequent Fault)

Fault Sequence Analysis

297 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.

298 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 SAPs FA.4 and FA.5. Since multiple redundancies are provided within the RPS, it is my judgement that the single failure criterion requirements of SAPs FA.6, EDR.2 and EDR.4 have been 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.

Method and Assumptions

299 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling the RCCA ejection fault, EDF and AREVA have made the following assumptions to ensure a robust and conservative assessment:

- the RCCA with the maximum worth is ejected including a 10% uncertainty allowance;
- the RCCAs are inserted to the maximum insertion limit;
- an ejection time of 0.1 seconds is assumed;
- a top peaked power distribution is assumed by modelling;
- a range of power levels are analysed;
- a range of burn-ups and fuel cycles are analysed;
- the fuel to coolant heat transfer coefficient is minimised; and
- the setpoint values include instrumentation and setpoint uncertainties and the maximum time delays are assumed within the analysis.

300 The EDF and AREVA analyses use the SMART and FLICA computer codes coupled together to model these RCCA ejection faults. The assessment of the SMART and FLICA computer codes against the validity of assurance SAPs FA.18 to FA.22 is reported in the Fuel and Core Assessment Report (Ref. 15).

301 These assumptions represent a fairly standard approach to the design basis analysis of such faults and are comparable to those applied in the Sizewell B analysis. They are judged to result in a bounding assessment meeting the requirements of SAP FA.7.

Transient Analysis

302 The analysis results are summarised in Table 2 of Chapter 14.5.5 of the PCSR (Ref.12) 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 control 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 RCCA is 135 pcm, the peak centre fuel temperature is predicted to be 1972ºC

and the maximum fuel enthalpy rise is predicted to be 391 J/g (93.1 Cal/g). The peak fuel enthalpy occurs at 42% power and is 487 J/g (116 Cal/g).

303 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. 52) as an exemplar of relevant good practice in the UK. The results of the EDF and AREVA analysis have been compared with the Sizewell B analysis 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 RCCA is predicted to be 116 pcm and the peak centre fuel temperature is predicted to be 1799ºC. The predicted fuel enthalpy is not quoted but it is stated to be significantly less than 588 J/g (140 Cal/g). These results give reasonable confidence in the UK EPR analysis since the peak centre fuel temperature scales with ejected RCCA worth. The EDF and AREVA results suggest that the RCCA 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. In response to TQ-EPR-1088 (Ref. 9), EDF and AREVA have confirmed that the RCCA limits assumed in this analysis include an additional allowance beyond that required for steady state operation to account for the need to perform limited load following due to potential perturbations in the grid.

304 It should be noted that as a result of RO-UKEPR-60 (Ref. 10), EDF and AREVA have been in the process of revising the Radial Averaged Peak Fuel Enthalpy (RAPFE) safety limit against which they assess their peak fuel enthalpy. This work has resulted in a revision of the transient analysis for this fault. The revised analysis, which has been incorporated into the latest version of the PCSR (Ref. 14), predicts that the worst enthalpy rise occurs at 82% power when the margin to the revised limits is 258 J/g. These revised limits and transient analysis performed in response to RO-UKEPR-60 have been assessed and are reported in the Fuel and Core Assessment Report (Ref. 15). This report concludes that a future licensee will need to further revise this fault analysis to demonstrate that the RCCA insertion limit is adequate to prevent any fuel entering the DNB condition. It also states that a future licensee will need to review these derived criteria for cladding failure in reactivity insertion faults in the context of the results of the relevant experiments in the CABRI research programme when these become available. These issues have been raised as an Assessment Finding, **AF-UKEPR-FD-08** (Ref. 15). Notwithstanding these comments, subject to a satisfactory response to the Assessment Finding, it is judged that a sufficiently bounding assessment has been made for the purposes of this GDA assessment to give confidence that the requirements of SAP FA.7 will be met.

4.2.6.8 Controlled State to Safe Shutdown State

305 EDF and AREVA argue that moves from controlled state to safe shutdown state for these reactivity and power distribution faults are bounded by the feedline break case. A slight exception is the boron dilution event since this defines the limiting performance of the EBS to avoid re-criticality following the decay of xenon. However, this claim ignores the fact that many of these events are more frequent than the feedwater system pipe break fault and so there is a need to demonstrate a diverse means of reaching the safe shutdown state. This issue has been raised as Action 9 under the GDA Issue **GI-UKEPR-FS-02**.

4.2.6.9 Radiological Consequence Assessment

306 SAPs FA.3 and FA.7 require that a radiological consequence assessment should be performed on a conservative basis for each design basis fault sequence that can lead to the release of radioactive material. A detailed review of the radiological consequence assessment methodology applied by EDF and AREVA to design basis faults is presented in Section 4.3 below. The conclusion of this review is that further substantiation and justification is still required as part of new site specific radiological consequence analyses, but it is my judgement that the current methodology presented in the PCSR (Ref.12) is broadly appropriate for this preliminary Step 4 GDA Assessment of individual faults against Target 4 in the HSE SAPs.

307 The PCSR argues that these reactivity and power distribution faults are bounded by the release from the PCC-2 loss of condenser vacuum fault with a single failure that results in the failure to isolate the MSRT since the steam releases will be almost equivalent. The releases from the condenser vacuum fault comfortably meet the Target 4 limit. In the case of the RCCA ejection event, EDF and AREVA claim that the radiological consequences meet the requirements for PCC-4 events, which included faults such as large LOCA which is predicted to result in a release of 0.08 mSv. Given the expected frequency for a PCC-4 fault, it is judged that the requirements of SAP Target 4 have been met.

4.2.6.10 Findings

308 Following my assessment of these reactivity and power distribution faults, I am broadly content with the fundamental design of the UK EPR to protect against this class of fault. In my judgement, the provision of in-core detectors connected directly to the RPS represents a significant safety improvement over the ex-core detectors that were provided on earlier generations of PWR designs. The development of this system, coupled with the reactor core's relatively low power density, should ensure adequate protection against most of the faults in this fault class.

309 I welcome the decision by EDF and AREVA to implement a modification to provide a high axial offset trip signal and a high neutron flux trip signal on the diverse protection system. These modifications represent a significant safety improvement in my judgement. Progress with these modifications will be monitored under the GDA Issue on diversity, **GI-UKEPR-FS-02** (Action 4). However, I consider that there is still a need for further evidence to be provided on the effectiveness of the diverse protection for RCCA misalignment faults at power and for boron dilution faults during shutdown conditions. These requirements have been identified as Action 5 and Action 7 of GDA Issue **GI-UKEPR-FS-02** respectively. In addition, I consider that there is also need for further evidence to demonstrate that for the RCCA bank withdrawal fault occurring at power, there is a diverse trip signal available for the full range of reactivity insertion rates and power levels (**AF-UKEPR-FS-15**) and that setpoints for the SAS system are sufficient to ensure that the fuel does not enter DNB (**AF-UKEPR-FS-16**). Finally, there is also a need to demonstrate adequate protection for boron dilution faults occurring at power with the control system in operation (**AF-UKEPR-FS-17**). While it is my judgement that these Assessment Findings are unlikely to result in design changes to the C&I systems on the UK EPR, the analyses performed in response should nevertheless be completed before the affected safety SSCs are delivered to site.

310 An Assessment Finding, **AF-UKEPR-FS-18**, has been raised with regard to the inadvertent loading of a fuel assembly in an improper position. This item will require

some analysis but is not considered to be a fundamental issue with the design and, in my judgement, can be closed out as part of the site licensing process before fuel is brought onto site.

4.2.7 Increase in Reactor Coolant Inventory Faults

4.2.7.1 Summary of EDF and AREVA's Safety Case

311 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.

312 The basis of EDF and AREVA's 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. They claim that the RPS is able to isolate the fault without the need for a reactor trip.

4.2.7.2 Assessment

313 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.

314 EDF and AREVA have identified this fault as a PCC-2 event and so it needs to be treated as a design basis event to meet the requirements of SAPs FA.4 and 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 is to be qualified to Class 1 (F1A) 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 fault, EDF and AREVA have reviewed this fault within the response to RO-UKEPR-41 (Ref. 46) and argue that it is adequately protected by CVCS isolation on high pressuriser level by either the RPS or the SAS system without the need for a reactor trip signal. Should these fail and the PSVs open then the event is bounded by the frequent small break LOCA transient.

Consequential Failures

315 In my GDA Step 3 Assessment Report I noted that no discussion is presented within the analyses about the possibility of consequential failures such as a stuck open PSV resulting in a consequential LOCA should the pressuriser become water solid. During GDA Step 4, EDF and AREVA have reviewed all the intact circuit PCC faults with the potential to lift the PSVs (TQ-EPR-947, Ref. 9). However, this event is not included as it should not result in the PSVs lifting.

4.2.7.3 Findings

316 I agree with EDF and AREVA that the consequences of this fault are adequately protected against.

4.2.8 Decrease in Reactor Coolant Inventory Faults

317 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); and
- 2A-LBLOCA.

318 The principal thermal hydraulic code used to assess all the faults identified above is CATHARE. This has been discussed in Section 4.2.8.9 after the individual faults and assessed against SAPs FA.17 to 24.

319 The general approach UK EPR design in response to a loss of RCS inventory (during at-power operations) is to detect a drop in pressuriser pressure, resulting in a reactor trip and the generation of a safety injection (SI) signal. This signal starts all MHSI and low head safety injection (LHSI) pumps injecting into the RCS cold legs. However, this needs to be accompanied by a deliberate partial cooldown to reduce the RCS pressure to within the delivery pressure range of the MHSI. The largest breaks will result in a pressure reduction without the need for a deliberate cooldown since the accumulator's delivery pressure will be reached (below the pressure level targeted with the partial cooldown). A subsequent cooldown (if needed, depending on the break size) reduces the RCS pressure further to within the range of the LHSI pumps.

320 In the longer term for smaller breaks, at least one of the LHSI pumps is switched from safety injection mode (SIS) to reactor heat removal mode (RHRS) to remove the core decay heat and the heat generated by the RCPs.

4.2.8.1 Summary of EDF and AREVA's Safety Case for SGTR

321 A SGTR is a small break in the RCS. It induces a depletion of the RCS water inventory and a depressurization of the RCS, the magnitude of which depends on the size of the break. The leak is partly or fully compensated on the primary side by operational systems, in particular the CVCS. On the secondary side, the pressure remains stable and the affected SG (SGa) level increases depending on the capacity of the controllers to stabilize the plant, in particular the Main Feed Water System (MFWS) or the Start-up and Shutdown System (SSS), and the plant power level. Due to the transfer of radioactive coolant into the SGa, the activity sensors in the SG blowdown, the main steam lines and the condenser will detect a higher level of radioactivity than in normal operation.

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

323 The approach of EDF and AREVA is to subdivide the transient into short term and long term phases 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 RCS injection. In the long term phase, the plant is transferred to safe shutdown conditions with a possible activity release if depressurisation of the affected SG by the MSRT is required.

324 In the November 2009 PCSR (Ref. 12), the design basis fault sequence for both the PCC-3 single tube rupture and the PCC-4 two tube ruptures occurring at full reactor power is described as follows. A reactor trip is assumed to occur on either a low pressuriser level or high SG level signal generated on 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 safety classified. It would also not be available following a 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.

325 The continuous loss of RCS coolant inventory causes the pressuriser to empty. Significantly, the PCSR assumes that this results in a depressurisation of the RCS because the CVCS is not able to match the break flow (an assumption that is no longer supported, see below).

326 Upon the receipt of a SI signal on either low pressuriser pressure or low SG level from the affected SG, the UK 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 RPS system decreasing the MSRT setpoint of the four SGs from 95.5 bara to 60 bara, at a rate giving a cooldown of 250°C/h (at the same time, the MSB setpoint is decreased from 90 bara to 55 bara at the same rate although this is not claimed in the analysis).

327 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 bara (see Ref. 53).

328 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.

329 From the controlled state, the affected SG is identified and isolated automatically. 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 pressures of the affected SG equalise, the flow via the break is terminated.

330 This is defined as the end of the short term phase; a state which Ref. 12 claims can be achieved using only automatic Class 1 (F1A) signals and systems.

331 The safe shutdown state is defined as a state where the affected SG is isolated and one SIS / RHRS train is connected to the RCS. To achieve the safe shutdown, the operator is required to initiate boration via the EBS and cooldown the RCS using the unaffected SGs. It is the transition from the leak termination to safe shutdown that EDF and AREVA examine with the long term phase of the transient.

332 At the end of the RCS cooldown, the RCS pressure (with the MHSI still on) is higher than the 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 classified 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.

333 The claimed systems and operator actions required to transfer to the safe shutdown state are all at least Class 2 (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.

334 Transient analysis is presented in Ref. 12 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 occurs (and therefore no liquid is released to the environment prior to leak termination).

335 The PCSR (Ref. 12) states that the cases without LOOP (for both PCC-3 and PCC-4 faults) are "new" calculations performed within the framework of GDA. They have been done with the CATHARE code for a 4500 MWth EPR.

336 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 (Ref. 12). The thermal hydraulic code S-RELAP5 has been used for this analysis and not CATHARE. 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 originally performed for the Flamanville 3 Preliminary Safety Analysis Report (PSAR) assuming a reactor power of 4250 MWth.

337 The description of the fault sequence following a SGTR event summarised above is assumed in Ref. 12 to be equally applicable for the PCC-3 single tube rupture and the PCC-4 two tube ruptures faults. However it was established during GDA Step 4 that the current UK EPR CVCS capacity is sufficient to compensate for a leakage up to more than a total guillotine break of a single SG tube. As a result, it is not possible to claim that a decrease of the RCS water inventory will be sufficient to trigger thermo-hydraulic protection signals. Similarly, the resulting increase in inventory in secondary side of the SGs can be compensated by a relatively small (~4%) reduction in MFWS flow when the plant is operated at full power. Therefore neither of the reactor trip signals on low pressuriser pressure or the high SG level can be assumed in the design basis safety case to be effective for the 2A-SGTR fault occurring at full power.

338 EDF and AREVA have recognised this and they have an on-going programme (CMF#22) to modify the design and update the safety case, with a reliance on detection of increased secondary activity levels to initiate action. The UK EPR November 2008 design freeze, which was assumed in the November 2009 PCSR (Ref. 12), did have activity monitoring which could detect SG leakages. However, this was not credited in the design basis safety case. Detection of activity would be carried out at the steam outlet lines and on the SG blowdown line. As originally proposed, there would be one N16 gamma detector per steam line. EDF and AREVA favour these detectors because of their sensitivity which allows very small leaks to be detected. However, they are larger than alternative designs (e.g. the detectors used on the SG blowdown line). Seismic limitations resulted in an original Class 3 (F2) safety classification for the activity monitoring system but EDF and AREVA have proposed to move the location of the SG blowdown water line detectors so that the system can be reclassified as Class 2 (F1B).

339 Claiming activity detection instead of the thermo-hydraulic protection systems, even after reclassifying the system to Class 2, would still not meet EDF and AREVA's own design

rules for PCC events to have Class 1 (F1A) systems to achieve the controlled state and leak termination. In Ref. 55, they have considered two further design options to address this shortfall: providing a second N16 detector on the steam lines combined with a manual reactor trip or installing four NaI scintillator detectors on each steam line to provide an automatic trip with 2-out-of-4 voting logic. The intention is that either option will result in a reactor trip via Class 1 means. EDF and AREVA state that the N16 detectors are too large for four to be installed in the space available. Their favoured approach is the first option of a manual reactor trip from two N16 detectors.

340 In Ref. 56, EDF and AREVA have reassessed the short term analysis of a single tube rupture from a pre-trip power of 102% (i.e. 4590 MWth) without LOOP assuming a manual trip (prompted by secondary side activity levels) 30 minutes after the break opens. The analysis also credits a number of other operator actions, including isolating the affected SG, raising the MSRT setpoint on the affected SG, stopping MFWS flow to all SGs, disabling EFWS flow to the affected SG and starting EFWS flow to the intact SGs. Ref. 56 predicts that 92 tonnes of steam will be discharged to atmosphere via the MSRT from the affected SG during the short term phase. The original short term analysis in Ref.12 predicted the release of 118.6 tonnes of contaminated steam to atmosphere.

341 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 combined steam release masses from the short and long term calculated from 102% power no LOOP analysis (from the two tube rupture fault analysis which is unaffected by the greater CVCS charging capacity), the PCSR presents effective dose values, for the notional limiting individual, not exceeding 170 μSv.

4.2.8.2 Assessment for SGTR

342 The assessment of SGTR faults can only be limited at this time. I have assessed the information made available to me, including the optioneering study of design changes to facilitate a trip on secondary activity. However, Refs 55 and 56 came in very late in GDA Step 4 and only partially address the matters of concern to HSE ND. EDF and AREVA still need to take the complete design change (CMF#22), encompassing both the change in the physical design and the change to the safety case) through the robust modification process, with a full impact assessment. This is therefore a GDA Issue, **GI-UKEPR-FS-04**, Action 1.

343 EDF and AREVA have stated that their preferred strategy for mitigating a PCC-3 single SGTR is to claim a Class 1 (F1A) manual trip on activity. The alternative design considered (2oo4 automatic trip) is similar to that adopted at the Olkiluoto EPR in Finland. In Ref. 55 EDF and AREVA have presented arguments as to why they prefer to utilise N16 detectors which are too large for 2oo4 tripping logic. The larger detectors allow them to follow an early management strategy of leaks that has been successfully adopted in the EDF French fleet, preventing the leaks from developing into the full 2A-tube ruptures. However, the arguments presented in Ref. 55 are restricted to the initial reactor trip. In addition to a manual trip, the revised mitigation strategy also requires the operator to perform additional manual actions (such as isolation of the affected SG and start of the EFW) to reach the controlled state. The equivalent actions in the original UK EPR design (and in the Olkiluoto design) are all automatic. In the PCSR (Ref. 12) these additional actions are identified as Class 2 (F1B). Therefore, from the evidence provided to date, the management of the PCC-3 SGTR fault does not meet EDF and AREVA's own design rule of relying on Class 1 (F1A) SSCs to reach a controlled state and leak termination. In addition, SAPs EKP.5 and ESS.8 set the expectation that automatically initiated

engineered safety measures should be used in preference to manually initiated engineered safety measures. In the response to Actions 1 and 2 of **GI-UKEPR-FS-04** EDF and AREVA need to provide more information on the safety classification of these manual actions and an ALARP argument as to why they propose not to automate these actions, even if it is accepted that an initial reactor trip prompted by N16 detectors needs to be manual.

344 Ref. 56 presents new transient analysis of a single tube rupture assuming the manual trip and subsequent operator actions discussed above. Until EDF and AREVA have provided further substantiation of the operator actions, it is difficult to be definitive on the acceptability of this analysis. It is noted that the operator actions of concern are all assumed to occur almost simultaneously 30 minutes after the break first opens. No justification for this is given and there is no discussion on whether failure to perform one of these actions successfully will change the fault sequence in a significant way. It may well be that failure of any particular action will prompt the series of automatic actions that were originally envisaged but no evidence for this has been provided. There is also no evidence that EDF and AREVA's assessment of the limiting single failure remains valid with the revised strategy.

345 It is recognised that (partially) removing the automation of SGTR faults management in the design basis safety case returns the design to an approach similar to that employed in operating PWRs.

346 The analysis in the PCSR (Ref. 12) to demonstrate a margin to overfill and that the safe shutdown state can be reached for a single tube rupture considers a single transient occurring from 2% power without LOOP. The N16 detectors proposed are not claimed to be effective below 20% power, while measurements of SG secondary side pressure and level can still be claimed at low power. Therefore this analysis could potentially remain appropriate. However the analysis presented in Ref. 12 does not consider the proposed UK EPR reactor design in the following ways:

- 4900 MWth is assumed rather than 4500 MWth;
- MHSI injection is assumed to have a delivery pressure 5 bar lower than for the 4500 MWth design;
- The CVCS charging flow is assumed to be 20 kg/s (less than the maximum break flow from a 2A-SGTR) compared to the 28 kg/s now identified as the charging flow capacity (more than the break flow from a 2A-SGTR);
- Manual isolation of the CVCS charging line is assumed after 30 minutes instead of the automatic isolation available in the 2008 design freeze;
- A partial cooldown rate of 100°C/h is assumed rather than 250°C/h.

347 While it is unlikely that the amount of active steam that is released to atmosphere will change significantly, these differences will have an impact on the timing of key stages within the fault transient. It is my view that the reactor design has diverged away from the analysis presented in the PCSR to such an extent that new analysis of the PCC-3 2A-SGTR event is required to demonstrate there is a margin to overfill and that the long term safe shutdown state can be reached with safety criteria met. Demonstrating that there is margin to overfill is principally about completing actions within a specific time. The divergence between the analysis and the design means that the timing of events in the transient is such that I cannot assess the analysis positively against the requirement of FA.17 for theoretical models to adequately represent the facility. The requirement to

reanalyse the fault with assumptions appropriate for the UK EPR has therefore been raised as Action 3 under GDA Issue **GI-UKEPR-FS-04**.

348 I accept that the safety case and transient analysis presented in the PCSR (Ref. 12) for two tube ruptures in the same SG (4A-SGTR) from a reactor initially at full power and with LOOP remains appropriate. The loss of inventory through the break is beyond the capacity of the CVCS (even with the higher charging capability in the latest UK EPR design) and therefore a reactor trip will be triggered by low pressuriser pressure. The 4A-SGTR analysis does not take into account partial cooldown rate of 250°C/h. However, in response to TQ-EPR-576 (Ref. 9), EDF and AREVA have demonstrated that the effect of an increase in partial cooldown rate is minimal on design basis SGTR analysis (full power cases, not the margin to overfill cases from low power) because the assumed single failure is the main steam relief control valve (MSRCV) of the affected SG stuck. The steam flow from the failed open MSRCV is so great that cooldown is accomplished using only the affected SG's MSRT. The actual cooldown rate exceeds both 100°C/h and 250°C/h for the first part of the partial cooldown phase and therefore the change in rate is not a significant parameter in the design basis analysis of the transient.

349 The demonstration that there is a margin to overfill for the 4A-SGTR suffers from the same shortfalls as the equivalent analysis for the 2A-SGTR fault; the presented analysis is old and now does not reflect the UK EPR design sufficiently for me to have confidence in the quantitative arguments presented. Therefore Action 3 of GDA Issue **GI-UKEPR-FS-04** also requires the reanalyse of the margin to overfill for the two tube rupture SGTR fault.

350 The PCSR (Ref. 12) does not consider multiple tube ruptures (more than two) within the design basis. The frequency attributed to a 4A-SGTR in the PSA is 2.0×10^{-4}/y (Chapter 15 of Ref. 12). While the simultaneous rupture of more than two tube ruptures in the same SG is expected to be even less frequent, initiating events with a frequency two orders of magnitude smaller could still be candidates for design basis consideration (EDF and AREVA include initiating frequencies down to 1×10^{-6}/y within PCC-4). In response to this issue being put to them via TQ-EPR-574 (Ref. 9), EDF and AREVA identified a number of mechanical aspects and precautions which they claim will limit the occurrence of multiple tube ruptures. In addition, they claim that the effect of increasing the number of broken tubes is only to accelerate the termination of the leakage, without occurrence of any cliff edge effects.

351 To support this last claim, EDF and AREVA have assessed the consequences of 10 tubes failing simultaneously in one SG with CATHARE (Ref. 57). Although this analysis makes many non-bounding assumptions (e.g. no single failures assumed, MSB assumed available), it supports their claim that the plant can be brought to the final safe shutdown state without violating safety criteria and that the effect of increasing the number of broken tubes is to hasten the termination of leakage. This is summarised in the revised March 2011 version of the PCSR (Ref. 14). I accept these arguments and consider the coverage of multiple tube ruptures in the March 2011 PCSR to be adequate.

352 In response to RO-UKEPR-41 (Ref. 21), EDF and AREVA identified that additional arguments are needed to those provided in the PCSR to demonstrate the tolerability of the UK EPR to a passive single failure of the transfer line between two partner SGs. This line provides a Class 2 means of decreasing the affected SGs water inventory to allow depressurisation and prevent overfilling. EDF and AREVA stated that the consequences of such a failure would not have a direct impact on radiological consequences outside of containment and that if it is assumed consistent with usual design basis analysis assumptions, then it would be considered in place of a more penalising single failure.

The effect of not having the transfer line (believed to be a new feature of the EPR) would be an increased risk of overfilling whereas the consequences of a break in the transfer line is a leak within containment, which is less onerous than the active single failure already considered. In identifying this potential vulnerability, I am satisfied that the requirement of SAP FA.6 to consider single failures has been met and I accept their arguments in Ref. 21 as to why the current design is ALARP.

353 As SGTR is a PCC-3 event, it is considered by EDF and AREVA in their response to RO-UKEPR-41 as a frequent fault (Ref. 45). However, they argue that the consequences of an ATWT event are bounded by the equivalent ATWT events for a SBLOCA fault. Likewise, the common mode failure of the MHSI or the partial cooldown will also be more onerous for a SBLOCA fault since the break size is larger and cannot be isolated. EDF and AREVA have provided an ALARP justification (Ref. 91) for not providing a diverse MSIV design. I accept this argument on the basis that failure of the MSIV to close following an SGTR fault will only result in an effective dose release in the range of 1-10 mSv (as calculated in the Level 3 PSA). There is also the precedent set at Sizewell B, which does not have a diverse MSIV.

354 The radiological consequences analysis presented in Chapter 14.6 of the PCSR (Ref. 12) are calculated from the 4A-SGTR analysis from 102% power and with LOOP. Both the short term and long term aspects of this calculation remain unaffected by the change in trip parameter for the PCC-3 2A-SGTR fault and my doubts associated with the low power margin to overfill calculations. Therefore, as long as the steam release assumed for this fault continues to bound that predicted for all other SGTR faults, the thermal hydraulic input assumptions in the radiological consequences analysis should remain valid. The details of the radiological assessment calculations are discussed further in Section 4.3 below.

355 My assessment of EDF and AREVA's analysis of consequential SGTR failures as a result of steam line break faults has already been presented in Section 4.2.2.

356 The principal code used to assess SGTR faults is CATHARE V2.5. This code is an advanced, two-fluid, thermal hydraulic computer code designed for use in realistic studies of accidents in PWRs. It provides a detailed representation of the primary and secondary sides. It is the same code that is used for the analysis of LOCA faults and therefore the assessment of CATHARE is deferred to Section 4.2.8.9 below.

357 Some of the (older) analyses presented in the PCSR were undertaken with S-RELAP5. Like CATHARE, it is well established thermal hydraulic code supported with a wealth of documentary evidence and test results. I have not assessed the validation of this code as part of GDA. It is expected that in addressing the GDA Issue and Assessment Findings associated with SGTR faults, the legacy S-RELAP5 analysis will be replaced with new CATHARE analysis.

4.2.8.3 Summary of EDF and AREVA's Safety Case for SBLOCA

358 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.

359 For the State A fault, a reactor trip is assumed to occur on low pressuriser pressure. The reactor trip signal automatically trips the turbine and closes the main feedwater system

lines. In the design basis analysis, a LOOP 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).

360 The SI signal is generated on low pressuriser pressure (at a lower pressure than the reactor trip low pressure set point) 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 RPS system to decrease the MSRT setpoint of the four SGs from 95.5 bara to 60 bar, at a rate giving a cooldown of 250°C/h.

361 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 Class 1 (F1A) systems.

362 The safe shutdown state is reached from the controlled state using Class 1 (F1A) and Class 2 (F1B) actions. The Class 2 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 is 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.

363 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 Class 3 (F2) CVCS can provide boration if it is available to compensate for the reactivity insertion resulting from the RCS cooldown. If the CVCS is not available, the Class 1 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.

364 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.

365 The PCSR (Ref. 12) argues that analysis undertaken for a 4250 MWth EPR 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 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.

366 The capability to reach a safe shutdown state is demonstrated using analysis for a 4900 MWth EPR design (Appendix 14B of Ref. 12) with similar assumptions to those made for the controlled state analysis. The core remains covered throughout the transient with the RCS 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.

367 The design basis assessments of SBLOCA are extended in the PCSR (Ref. 12) by considering individually the common cause failure of three safety systems through RRC-A best estimate accident analysis.

- 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 bara 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 bara 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.
- 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 83 minutes after the initial break (approximately one hour after the completion of partial cooldown) and the final state can still be reached with the identified LOCA acceptance criteria being met.
- SBLOCA without LHSI / RHR has been considered. With this system unavailable, EDF and AREVA claim that 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.

4.2.8.4 Assessment for SBLOCA

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

369 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 assessed but does not

seem unreasonable. 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.

370 In general, the approach and methodologies for considering SBLOCA PCC-3 events are the same as for the more challenging design basis IB/LBLOCA PCC-4. I have therefore deferred some of my assessment comments on SBLOCA to the assessment section below on IB/LBLOCA. However, during GDA Step 4 in response RO-UKEPR-57 (Ref. 10), the assessment of IB/LBLOCA PCC-4 events has been updated with the relevant PCSR section being updated accordingly (Ref. 14). The SBLOCA analysis (both PCC-3 and RRC-A) remains a mixture of 4250 MWth analysis assuming a partial cooldown rate of 100°C/h and assessed with CATHARE, and even older analysis assuming 4900 MWth and using S-RELAP5. Although I do not believe any safety limits are threatened, I believe it is necessary to make an Assessment Finding **AF-UKEPR-FS-19** for the analysis to be repeated with boundary conditions and assumptions specific to the UK EPR.

371 RO-UKEPR-41 (Ref. 10) required EDF and AREVA to demonstrate that the UK EPR has diverse systems capable of providing crucial safety functions following frequent faults (initiating event frequencies close to or greater than 10^{-3} per year). SBLOCA faults are amongst those considered in the RO response (Ref. 46).

372 EDF and AREVA have identified five fault sequences that need to be assessed to demonstrate that the UK EPR has diverse means of ensuring there is sufficient RCS water for core cooling:

- SBLOCA with ATWT event due to failure of RCCAs to insert;
- SBLOCA with ATWT event due to failure of RPS to trip the reactor;
- SBLOCA without MHSI;
- SBLOCA without partial cooldown signal; and
- SBLOCA with failure of containment isolation.

373 The third and fourth of these are already considered in the analysis of RRC-A events. In my opinion, this misses two sequences that also need to be considered:

- SBLOCA without partial cooldown (due to common mode failure of the MSRTs); and
- SBLOCA without LHSI.

374 The LHSI is required to move from the controlled state to the safe shutdown state. Although it is not considered within the RO-UKEPR-41 response, it is considered in the RRC-A analysis.

375 The SBLOCA with ATWT events have been considered in the response to RO-UKEPR-41 (Ref. 46). EDF and AREVA argue that the SBLOCA with ATWT due to failure of the RPS is bounded by the SBLOCA with ATWT due to failure of RCCAs to insert. Given that there is a diverse trip signal on low hot leg pressure and a diverse SI signal and partial cooldown signal on very low hot leg pressure, these arguments are accepted.

376 EDF and AREVA have performed explicit transient analysis for the SBLOCA with ATWT due to failure of the RCCAs to insert. The calculation is performed on a conservative basis. The RCCAs are assumed to fail to insert on the low pressuriser pressure trip signal at 79 seconds, causing the ATWT signal to be generated at 99 seconds. This trips

the turbine and actuates the EBS. The primary pressure and temperature increase causing boiling in the core at 120 seconds and the first PSV to open at 211 seconds. The boiling causes the reactor to go sub-critical, reducing the reactor power rapidly to decay heat levels. The turbine trip causes the SG level to fall resulting in the RCPs tripping on low SG level at 177 seconds. After 194 seconds the EFWS is actuated on very low SG level. As the reactor cools, the primary pressure falls and the SI signal actuates partial cooldown after 1055 seconds. The partial cooldown rate has to be controlled to ensure that while the MHSI is able to inject, the core does not cool too much to allow a return to criticality. MHSI commences after 1316 seconds. Partial cooldown is complete after 1508 seconds and the reactor pressure stops falling. The MHSI cannot match the break flow rate and so the inventory continues to reduce until the MHSI can provide sufficient flow. The pressure falls until the accumulators inject at 2588 seconds. Boron injection from the EBS, MHSI, LHSI and accumulators is sufficient to keep the core sub-critical. Decay heat is removed by the secondary side. The analysis demonstrates that all the LOCA fuel safety criteria are met with significant margins. However, it is important to understand the margins provided by the adopted partial cooldown rate to avoid recriticality while ensuring adequate cooling of fuel. For this reason, I am raising an Assessment Finding, **AF-UKEPR-FS-20**, requiring a future licensee to perform sensitivity studies to the cooldown rate.

377 In the case of the MHSI and partial cooldown signal common mode failures, the RO-UKEPR-41 analysis makes a number of different assumptions, notably conservative reactor conditions, including an initial power of 102% for a 4500 MWth reactor. For the SBLOCA fault without MHSI, the operator is assumed to perform a fast cooldown 30 minutes after the initial SI signal. The equivalent action in the RRC-A faults is assumed to occur at 83 minutes when the operator has established that core outlet temperature is greater than 350°C and there is no MHSI. Similarly, the RO-UKEPR-41 analysis for a SBLOCA without automatic partial cooldown signal assumes the operator manually initiates partial cooldown 30 minutes after the initial SI signal, while the RRC-A analysis waits till the core outlet temperature reaches 350°C at approximately 56 minutes. The other (potentially) significant change in assumptions is that the RO-UKEPR-41 analysis assumes a partial cooldown rate of 250°C/hr. No fuel uncovery or clad heat up is predicted for either of these faults with the assumptions made. Some limited heat up is predicted for the RRC-A event.

378 The RRC-A analysis makes generally non-bounding assumptions and assumes the lower power of 4250 MWth but predicts some clad heat up. This is because the assumed partial cooldown rate of 100°C/h delays the initiation of operator actions. Although the RO-UKEPR-41 analysis makes bounding assumptions and considers a higher powered 4500 MWth reactor, it predicts no fuel uncovery/clad heat up. It is not clear to me if this can principally be attributed directly to the benefits of an increase partial cooldown rate or due to the change in operator response time (30 minutes after the initial SI signal).

379 EDF and AREVA have provided an ALARP justification (Ref. 92) for not providing a diverse set of containment isolation valves. I accept this argument on the basis that failure of the containment isolation valves to close following an SBLOCA fault will only result in an effective dose release in the range of 1-10 mSv (as calculated in the Level 3 PSA, Chapter 15.5 of Ref. 12). There is also the precedent set at Sizewell B, which does not have a diverse set of containment isolation valves.

380 In their response to RO-UKEPR-41, EDF and AREVA do not analyse the case of SBLOCA occurring with common mode failure of the MSRTs to operate. Instead, they argue that the operator can manually depressurise the reactor using the PDS (effectively

performing a bleed and feed operation) and claim that the transient is bounded by the total loss of feedwater case presented in Section 4.2.3.5. This may well be correct, but I considered that they need to provide analysis to demonstrate that this is the case. For this reason, I raised TQ-EPR-1432, for EDF and AREVA to provide explicit analysis of the fault. In addition, I require them to justify the indications the operator would use to determine whether and when to perform the PDS depressurisation. In their response to TQ-EPR1432 (Ref. 9), EDF and AREVA have provided a demonstration that the operator can successfully perform the bleed and feed operation based upon measurements of low loop level (RPV level lower than bottom of hot leg) and meet the relevant fuel safety criteria. However, the response arrived too late to be included within the revised PCSR and so will need to be included in a future revision of the PCSR under GDA Issue, **GI-UKEPR-CC-02**. This claim also reinforces the need for the PDS to be upgraded to a Class 2 system in response to Action 5 of the generic GDA Issue, **GI-UKEPR-CC-01**, on categorisation and classification (Ref. 25).

381 Although EDF and AREVA have not considered the case of SBLOCA occurring with common mode failure of the LHSI to operate in their response to RO-UKEPR-41 (Ref. 46), they have analysed the case within their RRC-A analysis. The LHSI is not needed to reach the controlled state immediately following the fault but it is used to reach the safe shutdown state in the long-term. In the RRC-A analysis, EDF and AREVA claim that the safe shutdown state can be reached by using the SSS or the EFWS instead, together with either the MSRT or MSB to provide a partial cooldown on the secondary side. The MHSI, accumulators and EBS are used to maintain sufficient water inventory and to ensure the long-term control of reactivity on the primary side while the IRWST, CHRS, CCWS and ESWS are used to control the containment pressure and provide the ultimate heat sink. The analysis has been performed using the S-RELAP5 thermal hydraulics code coupled to the containment thermal hydraulics code COCO and has been performed for the 4900 MWth reactor design reported in Appendix 16B of the PCSR (Ref. 12). Since the key parameter will be the decay heat, this should be a reasonably bounding analysis, although there are some design differences in the containment cooling systems for the two designs and the RRC-A analysis nominally uses best estimate data. Under Action 9 of the GDA Issue **GI-UKEPR-FS-02** on diversity, EDF and AREVA are being asked to demonstrate in general that for frequent faults there is a diverse means of reaching the safe shutdown state and that all the systems claimed are appropriately classified.

382 For all but the oldest analysis, EDF and AREVA have shown that all the relevant SBLOCA safety criteria are met by using the CATHARE code. My assessment of the CATHARE code is in Section 4.2.8.9. However, it is relevant to note here that GRS, as part of its independent confirmatory analysis, benchmarked their ATHLET model of the UK EPR against EDF and AREVA's CATHARE model using the SBLOCA without MHSI RRC-A fault analysis presented in PCSR (Ref. 12). The GRS analysis (Ref. 58) using a different thermal hydraulic code is supportive of EDF and AREVA's assessment of the fault progression and the conclusion for the assumed boundary conditions that any fuel clad heat up will be modest. This independent work with ATHLET not only supports EDF and AREVA's specific conclusions for the RRC-A fault assessed, but also provides me with additional confidence in the CATHARE analysis of all SBLOCA faults.

4.2.8.5 Summary of EDF and AREVA's Safety Case for IBLOCA and LBLOCA

383 Intermediate breaks (equivalent area 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). A spectrum of breaks size between 45 cm^2 (∅ 75 mm) and 240 cm^2 (∅ 185 mm) has been considered in the RCP discharge pipe. The location of the break is a pessimistic assumption to maximise the mass discharge rate. In addition a SIS line break (390 cm^2 - ∅ 225 mm) located in the cold leg and a surge line break (2 x 830 cm^2 - ∅ 2 x 325 mm) located in the hot leg have been considered.

384 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. As part of the argument, the identified pipework is identified as a "High Integrity Component" with the highest M1 mechanical classification applied to it. As a result, the PCC-4 LBLOCA fault does not include a 2A-break of the hot or cold leg.

385 The initial sequence of events for the PCC-4 event, 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.

386 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.

387 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.

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

389 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.

390 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 circumstance, 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.

391 To achieve safe shutdown following larger 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.

392 The PCSR (Ref. 12) 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 is repeated at 4500 MWth (with the other assumptions unchanged) for the planned UK EPR reactor power. 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.

393 Although the PCSR (Ref. 12) states that this result supports the conclusion that there will be no cladding rupture and the core geometry will be maintained, my judgement at the end of my Step 3 GDA Assessment Report was that this had not been definitively demonstrated. However, the analysis had assumed a partial cooldown rate of 100°C/h while the planned cooldown rate for the UK EPR is 250°C/h. RO-UKEPR-57 required the EDF and AREVA to re-analyse the PCC-4 fault assuming conditions appropriate for the UK EPR, including the correct partial cooldown rate. This analysis is reported in Ref. 22 and has replaced the previously presented analysis in the March 2011 submission of the PCSR (Ref. 14).

394 In the updated analysis, a comprehensive spectrum of breaks has again been analysed. EDF and AREVA had initially considered the active failure of one EDG to start on demand following the fault. As a result, the MHSI pump, LHSI pump and one EFWS pump were assumed to be unavailable on the associated safety injection train. A second EDG was assumed to be unavailable due to preventative maintenance. With injection into the broken loop assumed to be lost out of the break, this results in one MHSI pump, one LHSI and three accumulators being available to inject into the primary circuit. At HSE ND's request, EDF and AREVA reassessed the break spectrum assuming the failure of a common SIS check-valve instead of the failure of an EDG to start (a second EDG was still assumed to be unavailable due to preventative maintenance). The consequences of the check valve failing to open are worse than the EDG failing to start because, in addition to the active systems being lost, the accumulator on the affected train is also unavailable. The result is one MHSI pump, one LHSI and two accumulators being available to inject into the primary circuit.

395 The most limiting peak cladding temperature predicted assuming the UK EPR's 250°C/hr partial cooldown rate is 763°C and is obtained for a 140cm^2 break with the failure of the common SIS check valve. Assuming the failure of the EDG (the "standard" single failure considered according to EDF and AREVA's own design basis analysis rules) results in a predicted peak temperature of 692°C, also for a 140cm^2 break. These temperatures are below the 1200°C peak fuel clad temperature limit and using the clad deformation model in CATHARE it is demonstrated that the maximum hot rod cladding deformation remains negligible throughout the transient.

396 The PCSR (Ref. 12) presents a second assessment to demonstrate that the safe shutdown state can be reached using only Class 1 (F1A) and Class 2 (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 EDGs 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.

397 IB and LBLOCA faults in shutdown State B are discussed in the PCSR but I have chosen not to sample this area of the safety case in the Step 4 review.

4.2.8.6 Assessment for IB and LBLOCA

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

399 The approach adopted appears to capture and bound all potential LOCA up to the largest pipe connected to the RCS loop. The assessment of the High Integrity Component (HIC) envelope and EDF and AREVA's break preclusion arguments which support the claim that a guillotine break of the main RCS pipework is beyond design basis is a significant area of focus for the Structural Integrity Assessment Report (Ref. 59).

400 The fault sequences for the different break sizes are clearly described. The analysis assumes a coincident LOOP and the unavailability of systems due to the limiting single failure and preventative maintenance are considered. With the updated analysis, it has not only been shown that the design can tolerate EDF and AREVA's standard limiting failure of one EDG but also the more onerous failure of a common SIS check valve (considered at HSE ND's request).

401 The PCSR presents supporting transient analysis to justify the claim that a controlled state can be reached with just automatic Class 1 (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.

402 I am therefore satisfied that the safety case presented for IB and LB LOCA faults is consistent with SAPs FA.4, FA.5, FA.6 and FA.9.

403 These faults fall naturally into two classes: those which depressurise of their own accord (some of which cause the inventory to flash and the vessel to empty); and those which require secondary depressurisation.

404 Considering the latter class, the peak cladding temperature predicted by the limiting calculation in the November 2009 PCSR for 80 cm^2 case was 825°C. The updated analysis presented in Ref. 22 for the same break size shows that assuming the 250°C/hr partial cooldown rate proposed for the UK EPR has a significant effect on this particular case; very limited and short lived core uncovery with a peak cladding temperature of 406°C.

405 With the quicker partial cooldown rate, Ref. 22 shows that 140cm^2 is the limiting break size. Even with a common SIS check valve considered, the predicted peak cladding temperature and clad deformation are stated to be acceptable. This is a welcomed but significant claim for the UK EPR. The thermal hydraulic code CATHARE has been used

to come to this conclusion. My assessment of CATHARE is given in Section 4.2.8.9 below. However to gain further confidence in the EDF and AREVA's modelling of the LOCA faults, I commissioned ISL to undertake independent confirmatory analysis of the spectrum of breaks considered in the RO-UKEPR-57 response.

406 US NRC is currently assessing the version of the EPR proposed by AREVA for the USA. To assist with this assessment, they have developed a thermal hydraulic model of the US EPR for fault analysis using the TRACE code. US NRC provided HSE ND with a copy of their US EPR LOCA model which was passed on to ISL to allow them to start their analysis from an advanced position. ISL modified the US EPR model to reflect the relatively minor differences in design of the UK EPR (Ref. 60) and then re-assessed the spectrum of breaks considered by EDF and AREVA for RO-UKEPR-57 with the same boundary conditions and single failure assumptions (Ref. 61).

407 The TRACE analysis predicts no core dryout and no fuel clad heat up for breaks in the RCP discharge pipe. The TRACE and CATHARE predictions for the individual breaks are very similar to the end of partial cooldown. However, the TRACE models go on to show that the loop seals (the U-leg piping between the SGs and the RCPs) clear of liquid. As the loop seals clear, the pressure buildup between the core and the loop seals due to core boiling is relieved. The resulting rapid drop in the primary system pressure allows the pressure for accumulator injection to be reached. In the CATHARE analysis, the delay in loop seal clearing is such that core uncovery has started before the accumulator injection point (at which the process of recovering liquid level in the core starts). In the TRACE analysis, the modelling of loop seal clearing is such that all the loop seals clear relatively early allowing the accumulators to inject before core uncovery has started and therefore avoiding clad heatup.

408 Loop seal clearing is notoriously difficult to model correctly and the effect is binary; it either happens or it does not. Both codes can point to validation to support their modelling of loop seal clearing (for TRACE see Section 4.94, BETHSY Test 6.2TC, Ref. 60, for CATHARE see ECHTOR tests identified in Refs 71 and 74). It does illustrate the importance of undertaking independent confirmatory analysis before taking predictions of such complex phenomena at face value. The TRACE and CATHARE codes (and GRS's ATHLET code) are all regularly employed in international benchmark comparisons against problems on test facilities and operating stations. Should a problem emerge in the future with any of the codes, it is anticipated that it would be rapidly identified and fixed. However, at present both TRACE and CATHARE are qualified for use in LOCA modelling and both predict (despite their differences) that the assumed design of UK EPR meets all of EDF and AREVA's deterministic safety criteria for a PCC-4 LOCA event.

409 The TRACE analysis does predict some limited clad heat up for the large SIS line break ($390cm^2$) during the initial seconds of the transients. This prediction, which is still not a threat to safety criteria, can be attributed to the simplified modelling of the reactor power post-trip. With the conservative assumptions made on reactor times and decay heat fall off, at the time of clad heat up the reactor power is still at a large fraction of nominal full power. If core power had been computed with more sophisticated reactor kinetics in the TRACE simulation, it would have resulted in an earlier and more rapid decrease due to voiding in the coolant.

410 ISL performed a sensitivity case for the 140 cm^2 break assuming a partial cooldown rate of 100°C/hr. This change caused the predicted primary pressure to remain higher, thus delaying the timing of safety injection actuation, resulting in a lower core level and a fuel clad temperature excursion. The peak temperature predicted was about 510°C. A

recalculation of the peak clad temperature for the 390 cm^2 break case assuming the lower partial cooldown rate showed little sensitivity to the change in rate. This is because the break size is large enough that the energy removal across the steam generators is much less than the energy leaving the break; therefore the cooldown rate has little effect on the fuel clad behaviour. However, for a range of intermediate break sizes, both EDF and AREVA's CATHARE analysis and ISL's TRACE analysis show that the partial cooldown rate is an important parameter. The UK EPR design employs MHSI pumps rather than HHSI pumps so the pressure in the primary system has to be brought down quickly for a range of break sizes for sufficient coolant to be added so as to minimise core uncovery. While it appears an acceptable case with significant margins on safety limits could be made for lower power EPR designs (e.g. 4250 MWth) with 100°C/hr, for the 4500 MWth proposed for the UK EPR, the faster 250°C/hr partial cooldown rate is necessary.

411 As a result of the revised analysis provided in Refs 22 and 14 and informed by ISL's independent TRACE work, I am satisfied that EDF and AREVA have assessed the consequences of this fault (during the crucial initial phases) in an appropriate way and shown on a conservative basis that the consequences are acceptable in accordance with SAP FA.7.

412 The analysis presented to show that the safe state can be reached for the limiting PCC-4 LOCA fault (the 390cm^2 SIS line break) is old, originally having being performed for an early 4900 MWth design. In response to TQ-EPR-1318 (Ref. 9), EDF and AREVA stated that despite some design and codes changes, they still consider the results presented in the PCSR bounding for the UK EPR. As a result, they have not proposed any updated analysis in the frame of GDA but stated an intention to provide UK specific studies later during the detailed design and nuclear site licensing phases, potentially using more advanced methodologies.

413 The PCSR clearly states the assumptions made in the analysis, the limiting fault has been considered, single failures are discussed and identified, the criteria for the analysis are set out and conservative boundary conditions are assumed (most obviously, a higher reactor power).

414 Given that it is expected to be replaced by new analysis specific for the UK EPR in the future, I have chosen not to assess in detail the coupled CATHARE/CONPATE calculation, accepting EDF and AREVA's claim at face value that the available results are bounding. However, I have raised an Assessment Finding **AF-UKEPR-FS-21** to ensure that the commitment given in the TQ to reassess the limiting fault (which is part of the basis for me not assessing the methodology in detail against SAPs FA.17 to FA.24) is completed in a later phase.

415 The offsite dose predicted for a PCC-4 LBLOCA (bounding IB and SBLOCA) is significantly less than 1 mSv. This calculation includes an assumption of a cladding failure fraction of 10% despite no core damage being predicted (damage is assumed to occur, without specific analysis, as a result of DNB). This would seem to be compatible with the numerical targets in the SAPs (Ref. 4) although the details of the radiological assessment calculations are discussed further in Section 4.3.

416 The analysis of PCC-4 LOCA faults is essential to demonstrate the acceptability of the significant UK EPR design feature of MHSI. It therefore places sizing requirements on the MHSI pumps. EDF and AREVA provided me with a copy of the 4500 MWth sizing report (Ref. 53) which redefines the sizing of mechanical equipment from that originally established for an early 4900 MWth reactor design. This defines the MHSI

characteristics (minimum required injection flow versus RCS pressure). Ref. 53 states these characteristics (identified as "RF002 MHSI") are acceptable, assuming an 80cm^2 break is the limiting fault with a partial cooldown rate of 100°C/hr. RO-UKEPR-57 has assumed the "RF002 MHSI" minimum pump characteristics (Figure 1 of Ref. 22), as has the ISL confirmatory work (Ref. 61). Both demonstrate that the characteristics are still acceptable with an increased partial cooldown rate, a larger limiting break size and a more onerous single failure assumption (i.e. a common SIS check valve failure). Therefore, the link between design basis analysis and the engineering requirements of the MHSI is retained, which is in accordance with FA.8 and FA.9.

417 The desired cooldown rate is achieved by the Class 1 (F1) RPS C&I altering the pressure setpoints on the MSRT control valves. During discussions with EDF and AREVA during GDA Step 4, it was established that the RPS compares the measured pressure against 24 pre-calculated points provided to it. EDF and AREVA stated that these calculated points will be checked by commissioning tests. Although I have not assessed in any further detail how the important parameter of partial cooldown rate will be ensured, I am satisfied that it is being achieved with Class 1 systems with all the requisite integrity such a safe classification ensures.

418 The design of the MSRT valves which facilitates the partial cooldown is based upon experience from the German Konvoi reactors and the French N4 reactors. This design has been discussed in the Mechanical Engineering assessment of the UK EPR (Ref. 64).

419 LBLOCA is traditionally used to sizes the accumulators. In this case, the requirement to demonstrate the design capability for the 2A-LBLOCA means that satisfactory design basis analysis is a necessary, but not a sufficient condition. 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.

420 There is little evidence presented on how the ALARP principle is applied to LOCA faults. 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.

4.2.8.7 Summary of EDF and AREVA's Safety Case for 2A-LBLOCA

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

422 The function of the engineered safety systems in this fault is to refill the reactor vessel and reflood the core before fuel damage occurs. Release of radionuclides in this event can be limited provided that the fuel can be demonstrated to remain within the conventional thermal design limits, so my focus has been on compliance with these thermal design limits.

423 Although EDF and AREVA have identified a HIC envelope which excludes consideration of failures of the main primary-circuit pipework within the PCC design basis, an assessment of a double-ended (2A) guillotine failure has still been made to demonstrate the capability of the design to withstand the fault and to justify that the fault is successfully protected for the purposes of PSA. This analysis provides the demonstration that the emergency cooling systems are functionally capable of responding to the fault and therefore the 2A-LBLOCA does not contribute disproportionately to the plant's risk of large radiological releases.

424 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 in Ref. 65.

425 The objective is to demonstrate that a coolable geometry is maintained in the fuel assemblies and that the amount of hydrogen released into containment is sufficiently low that it does not present a risk of fire damaging the containment structure.

426 These design requirements transpose directly to constraints on cladding surface temperature required to prevent excessive cladding oxidation, but recent analysis has also been able to demonstrate that few, if any, of the fuel pins would be expected to fail by clad ballooning. This analysis demonstrates, in a straightforward way, that fuel geometry will remain acceptable.

427 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.

428 The calculations are made using the CATHARE computer code, which is capable of representing 2A-LOCA on a best estimate basis with due allowance for modelling uncertainty.

4.2.8.8 Assessment for 2A-LBLOCA

429 I have assessed the 2A-LBLOCA against SAPs FA.15 and 16, which require a demonstration that no sudden escalation in risk occurs for faults excluded from assessment within the Design Basis and also against SAP EKP.3 which requires consideration of severe accidents as part of a strategy of defence in depth.

430 The general approach to selection of LOCA faults for assessment within and outside the design basis is considered reasonable, provided that the integrity claims for the main pipework can be substantiated. However, the assessment of the worst conceivable break configuration to demonstrate a design capability, provides additional comfort that plant risk is not unduly sensitive to the pipe structural integrity arguments. Furthermore this analysis is important for substantiating the assessment of plant risk and designing safety systems.

431 I have examined the analysis of core cooling in some detail because the case makes the novel (and very welcome) argument that the mean rod in the lead assembly will remain below cladding temperatures likely to cause clad failure by ballooning.

432 I have not examined the issue of depressurisation forces on reactor internals because provided that fuel does not balloon, I judge (consistent with the Sizewell B safety case) that there is not a significant risk of loss of coolable geometry within the fuel.

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

434 The cladding temperature reported in Ref. 66 is demonstrated to remain sufficiently low that burst is avoided. This is a significant improvement over current designs.

435 The assessment 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.

436 EDF and AREVA have modelled the response to the fault assuming reasonably bounding radial form factors.

437 I have examined the analysis results and on the basis of the temperature response, the initial fuel pressures and the alpha-phase creep of the cladding detailed in Ref. 63. I concur that extensive clad ballooning or failure of defect-free fuel rods is unlikely.

438 I also note that recent measurements of fission gas release from failed pins in experiments designed to simulate this fault has been lower than I expected (Ref. 67).

439 After the fault has reached a controlled state, operator action is required to ensure continued supplies of water for safety injection. This involves realigning pumps to draw from the containment building sump. The time available is similar to that of Sizewell B.

4.2.8.9 The CATHARE Computer Code

440 The CATHARE V2.5 is the principal code used by EDF and AREVA to model the depressurisation of the reactor primary cooling circuit following LOCA and SGTR faults. CATHARE is also used to model loss of feedwater events.

441 The physical modelling within CATHARE is detailed in Refs 69 and 70.

442 The code contains a number of empirical models that are tuned to realistically represent the performance of a set of separate-effect tests. The overall performance has then been tested in integral tests where a scaled representation of the facility has been used as required by SAP FA.18. These test matrices have been systematically derived in line with Organisation for Economic Co-operation and Development/Committee on Safety of Nuclear Installations (OECD/CSNI) recommendations (Ref. 71) and appear to be fit for purpose. The system performance is generally well represented.

443 The code represents the heat transfer to liquid and vapour in the primary circuit and steam generators by discrete sets of coupled equations. These allow for departures from thermal equilibrium appropriately and represent the fluid flows using a set of empirical rules, backed up by an extensive body of experimental data. The approach is consistent with that used elsewhere – notably in the US NRC sponsored codes RELAP and TRACE.

444 The prediction of fuel temperatures is dependent on: determining the precise time at which the fuel surface heat flux exceeds a critical value, causing the fuel to dry out; and then later, on the supply of water droplets to cause rewetting.

445 The prediction of the critical heat flux is based on tabulated experimental data and performs well over a wide range of conditions. The droplet modelling is based on a set of correlations, which do not fully represent the behaviour of droplets in a flow, but can be expected to represent the macroscopic trends within the region of applicability demonstrated for the model.

446 The dry fuel surface heat transfer is modelled using a simple function of Reynolds Number and Prandtl Number, based on bulk fluid properties. The effect of the thermal boundary layer temperature is neglected in this, resulting in a potential under prediction of cladding temperature, which would increase as the clad temperature limit was approached. However, the correlation also omits to account for the rod-bundle geometry and this factor more than compensates, so I judge that these errors combined are small compared to other uncertainties.

447 I judge 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 large LOCA and is of less significance in small LOCA. To obtain further confidence that the applied tuning was specific to the case of the UK EPR LBLOCA, I carried out some limited confirmatory analysis, which modelled the heat transfer within the fuel. This work does not constitute a formal validated study, but results were in reasonable agreement with those of CATHARE and help to support my view that the code is fit for purpose.

448 Other important models in CATHARE include the representation of entrainment in stratified flows and the prediction of sonic velocity. The models used are derived from experiments designed to test separate effects and the overall system performance is confirmed by integral tests. A subset of this validation work is reported in Ref. 71.

449 The CATHARE models seem to perform as well as alternative codes. CATHARE has been used as part of international benchmark exercises for many years and this has helped build confidence in its validity. The most relevant recent studies of the overall uncertainty associated with the code are found in the “Best Estimate Methods – Uncertainty and Sensitivity Evaluation” (BEMUSE) programme assessment (Ref. 72). This CSNI programme compared predictions of a number established LOCA assessment codes. The assessments included not only uncertainty studies using the Monte-Carlo method and Wilkes’ distribution-free assessment of uncertainty, but also an internal assessment of uncertainty based on experimental data (Ref. 72). The CATHARE predictions were consistent with the experimental data and the predictions of other codes.

450 As has been discussed in other sections of this report, as part of GDA Step 4 HSE ND has commissioned independent confirmatory analysis for smaller LOCAs with the ATHLET and TRACE thermal hydraulic codes. While inevitably there are some differences in the details of the predictions with different codes, none of the TSC work (Ref. 58 and 61) has undermined conclusions reached by EDF and AREVA using CATHARE.

451 CATHARE has a model of the effect of blockage on the coolant flow post fuel-pin failure by clad ballooning. The effect of the blockage on heat transfer appears to be represented reasonably enough (Ref. 69), but the analysis determining the level of blockage itself appears too simplistic. However, this issue has not become significant because the calculations presented for the PCSR indicate that extensive fuel failures can be precluded for the planned core loadings and the margins to fuel safety limits predicted are large.

452 The methodology used to demonstrate the margin to cladding failure is detailed in Ref. 73. This uses simulation of the deformation of limiting rods at the end of a cycle of operation (when pin pressures are a maximum). The limiting conditions are confirmed by an assessment of through-cycle core radial power profiles which demonstrates that the average assembly ratings remain below those of the postulated limiting rods. The approach retains a small amount of conservatism in assumptions on initial conditions. The approach is reasonable in the context of a demonstration of design capability. In the

case of the design basis faults, the margins to failure are sufficiently large not to require detailed justification.

453 I judge that CATHARE meets the requirements of SAP FA.17 and 18, i.e. that the models should adequately represent the facility and the processes.

454 The user of the code is provided with well structured user guidance (Refs 74 and 75) which meets the requirements of SAP FA.21.

455 The PCSR (both Ref. 12 and 14) still contains some older analysis undertaken with S-RELAP5. Like CATHARE, it is a well established thermal hydraulic code supported with a wealth of documentary evidence and test results. The validation of this code has not been assessed as part of GDA. None of the S-RELAP5 analysis in the November 2009 PCSR assumes 4500 MWth, a partial cooldown rate of 250°C/hr or the increased CVCS charging capacity. As part of the Assessment Findings to consolidate all the analysis with assumptions appropriate for the UK EPR, the S-RELAP5 analysis will be replaced by new CATHARE analysis. I therefore have chosen not to assess the S-RELAP5 against FA.17 to FA.24 for the UK EPR.

4.2.8.10 Findings

SGTR

456 The safety case for SGTR faults has been subject to significant change during GDA Step 4. EDF and AREVA need to provide more evidence to justify the claims made in their current strategy which relies heavily on manual actions in contrast to alternative strategies which compare favourably with SAPs EKP.5 and ESS.8.

457 Through Actions 1 to 3 of GDA Issue **GI-UKEPR-FS-04**, they need to establish a final justified management strategy and design, and provide analysis and modification submissions to reflect the outcome. Some old analysis, unaffected by the planned design changes to reactor tripping, still needs to be updated to reflect the current UK EPR design.

458 A thorough assessment of the SGTR design basis therefore cannot be completed at this time.

SBLOCA

459 The methodology employed to assess PCC-3 SBLOCA faults is essentially the same as that used for the more onerous (but less frequent) PCC-4 IB/LB LOCA faults and therefore I chose to concentrate my detailed assessment of methodology on the larger breaks.

460 In their response to TQ-EPR-1432, EDF and AREVA have demonstrated that manual operation of the PDS is functionally capable of providing diversity following a SBLOCA with common mode failure of the MSRTs. However, this response was provided too late to be included within the revised PCSR. The inclusion of such responses in future revisions of the PCSR is required under the cross-cutting GDA Issue, **GI-UKEPR-CC-02**.

461 An Assessment Finding, **AF-UKEPR-FS-19**, is placed on a future operator to update the SBLOCA transient analysis to more closely match the proposed UK EPR design but this is not expected to alter EDF and AREVA's claims on the acceptable consequences resulting from a SBLOCA fault. A second Assessment Finding, **AF-UKEPR-FS-20**, has been raised for the margins provided by the assumed partial cooldown rate to be

investigated following a SBLOCA with an associated ATWT event. Both of these Assessment Findings should be completed before affected safety SSCs are brought onto site.

IB and LB LOCA

462 As a result of the revised analysis performed for RO-UKEPR-57, which has considered a range of break sizes and limiting single failures, I am satisfied that EDF and AREVA have demonstrated the requirements of FA.4, FA.5, FA.6 and to FA.8 for PCC-4 LOCA faults on the UK EPR.

463 I note that independent analyses with two modern codes, CATHARE and TRACE, have predicted no fuel damage due to clad heat up for these break sizes. While I have no strong reasons to favour one code over the other, EDF and AREVA's code appears to be the more conservative of the two. I am therefore also satisfied that EDF and AREVA have met the requirements of FA.7.

464 An Assessment Finding, **AF-UKEPR-FS-21**, is placed on a future licensee to provide updated analysis of the limiting break size to show that safe shutdown state can be reached.

2A-LBLOCA

465 Double-ended guillotine breaks on the hot and cold legs are outside the PCC design basis and have therefore been assessed against the severe accident SAPs FA.15 and FA.16. I am satisfied that the requirements on these SAPs have been met and the risk from 2A-LBLOCA faults is ALARP.

CATHARE

466 CATHARE is a modern thermal hydraulic code that is well documented and validated, and has been shown to perform well in international benchmark exercises against alternative codes. As a result of my assessment, I am satisfied that CATHARE meets the requirements of FA.17 to FA.24.

467 Independent analysis undertaken for HSE ND during GDA Step 4 by ISL and GRS using alternative codes has been sufficiently confirmatory of the predictions and claims made by EDF and AREVA in the PCSR using CATHARE analysis.

4.2.9 Support System Faults (including loss of cooling chain)

4.2.9.1 Summary of EDF and AREVA's Safety Case

468 Faults in this category result in the loss of essential support systems on the reactor. These faults include loss of CCWS, loss of the ESWS, loss of the CVCS, and the loss of the HVAC system.

469 These faults are generally considered under the consequences of the fault and presented in the other sections. However, there are some failures that produce consequences that do not readily fall into other categories because the failure can result in multiple consequences. For example. the loss of the CCWS can result in loss of cooling the RCP seals causing a SBLOCA and failure of cooling to the IRWST with consequential loss of the MHSI.

470 As noted in their response to RO-UKEPR-40 (Ref. 26), EDF and AREVA are still in the process of developing a design basis safety case for a number of these systems.

4.2.9.2 Assessment

471 In their response to RO-UKEPR-40 (Ref. 26), EDF and AREVA have acknowledged that they still need to develop a design basis safety case covering loss of cooling chain systems (CCWS, ESWS) and loss of the HVAC system. Given the importance of these systems, a GDA Issue, **GI-UKEPR-FS-05**, has been raised requesting EDF and AREVA to provide a design basis analysis covering the loss of these systems. EDF and AREVA are to demonstrate the functional capability of the systems that protect against such faults and that they have an appropriate safety functional categorisation and linked safety system classification.

4.2.9.3 Findings

472 GDA Issue **GI-UKEPR-FS-05** has been raised requesting EDF and AREVA to provide a design basis analysis of failures in the essential support systems.

4.2.10 Control and Protection System Faults

4.2.10.1 Summary of EDF and AREVA's Safety Case

473 Faults in this category result in spurious operation of either the control systems or the protection systems on the reactor. In the case of the control system, the control loops potentially affected include power, pressure, pressuriser level, SG pressure and SG level control systems. In the case of the RPS, the faults cover spurious initiation of engineered safety features on the reactor such as spurious SI signal, spurious RCP trip, spurious feedwater isolation, spurious turbine trip, spurious steamline isolation and spurious containment isolation.

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

475 As noted in their response to RO-UKEPR-40 (Ref. 26), EDF and AREVA are still in the process of developing a design basis safety case for many of these systems. In particular, the design basis assessment of the control and limitation functions within the RCSL system is outside the scope of the GDA assessment.

4.2.10.2 Assessment

476 EDF and AREVA have considered spurious initiation of either pressuriser sprays or heaters as PCC-2 events meeting the requirements of SAPs FA.4 and FA.5. Protection is provided by the RPS which trips the reactor on low or high pressure. These events are frequent events and so EDF and AREVA have reviewed them as part of their response to RO-UKEPR-41 (Refs 45 and 46). They argue that failure to trip following spurious initiation of the pressuriser heaters will result in the PSVs opening. They claim this fault is bounded by other more onerous transients such as the spurious closure of the MSIVs with common mode failure of the PSVs, a judgement I am prepared to accept.

477 In the case of spurious operation of the sprays, EDF and AREVA have explicitly modelled the two ATWT events corresponding to RCCAs failing to insert and failure of the RPS to trip. These transients initially lower the primary pressure and so challenge the margin to DNB. In the case of the RCCAs failing to insert, the tripping of the turbine causes a heat-up transient that compensates for the initial fall in pressure and effectively transforms the transient into a turbine trip/loss of main feedwater ATWT event. The failure of RPS to trip is more distinct since the reactor is not tripped until the low hot leg pressure signal on the SAS system is reached after 188 seconds. In both cases there remains a large margin to DNB limit comparable to that for the loss of off-site power ATWT event.

478 Initiating events due to failures of the RCSL system are outside the scope of this GDA assessment. Ultimately, a future licensee will need to demonstrate that any failures associated with this system are either bounded by other design basis initiating events or provide explicit design basis analysis as part of the safety case for implementing the system on the reactor design.

479 The RPS is capable of spuriously initiating reactor trip, turbine trip, MFWS isolation, MSIV isolation, RCP trip, EFWS actuation, EFWS isolation, MSRT opening, MSRT isolation, MSRT setpoint increase, SIS actuation, Partial Cooldown, CVCS isolation, LHSI/RHR isolation, PSV opening, and containment isolation. In TQ-EPR-1089 (Ref. 9), EDF and AREVA were requested to demonstrate that these spurious actuations were already covered by the existing design basis analysis. Given that the cause of such a malfunction is failure of the RPS, EDF and AREVA were requested to assume that the RPS was unavailable to provide protection against its own spurious actuation. In other words, EDF and AREVA were asked to demonstrate that a suitably qualified diverse means of protection exists for such faults.

480 In their response to TQ-EPR-1089 (Ref. 9), EDF and AREVA have systematically reviewed spurious actuation of each of the engineered safety actuation signals on the RPS. In most cases they are able to argue in a straightforward manner that the event is either benign or that it is already covered by an ATWT transient due to failure of the RPS to trip. For example, MFWS isolation is covered by the loss of normal feedwater ATWT event. There are a couple of exceptions, spurious EFWS actuation and CVCS isolation. Spurious EFWS actuation results in a high SG level signal on the SAS system which isolates the MFWS resulting in the loss of normal feedwater ATWT event. Spurious CVCS isolation of the charging line results in a drop in pressure until a diversified trip occurs on hot leg pressure low. EDF and AREVA argue that the transient is then covered by the spurious pressuriser spray ATWT event. While I accept these arguments, there is still a need for a future licensee to formally consider spurious C&I signals as potential initiating events within the PCSR. For this reason, Assessment Finding **AF-UKEPR-FS-22** has been raised.

4.2.10.3 Findings

481 In response to **AF-UKEPR-FS-22**, a future licensee shall provide a safety case covering initiating events caused by spurious C&I actuation signals within the PCSR.

4.2.11 Spent Fuel Pool Faults

4.2.11.1 Summary of EDF and AREVA's Safety Case

482 The design of the spent fuel pool racks and cooling system is described in the PCSR (Ref. 12). In addition, the requirements for spent fuel cooling are set out in the system design manual (Ref. 76).

483 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.

484 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.

485 The spent fuel pool purification and cooling system Spent Fuel Pool Purification System / Spent Fuel Pool 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.

486 The FPCS comprises 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.

487 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 SBO diesel generator.

488 The two main FPCS trains are classified Class 2 (F1B). The third train is classified Class 3 (F2).

489 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.

490 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.

491 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.

492 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.

493 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.

494 Design basis spent fuel pool faults are considered in the PCSR (Chapter 14) alongside reactor faults. They are also described in the Fault Schedule (Ref. 24). 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.

495 The loss of one train of FPCS during normal reactor power operation is identified as a PCC-2 design basis transient. Both EOC and 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.

496 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).

497 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.

498 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.

499 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 from 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.

500 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.

501 The total loss of the two main cooling systems during shutdown for refuelling is identified as a RRC-A event. The cause of such a fault could be station blackout (off-site power supplies and the 4 EDGs) or the total loss of the cooling chain (a failure of all four trains on the CCWS and/or ESWS). In such a scenario, the independent third FPCS train is started up and takes over the role of removing the decay heat from the spent fuel pool. It is assumed that after local realignment, the third FCPS train is started manually from the control room when the pool temperature reaches 95°C. The design of the third train is such that the temperature will not increase above 95°C and will be stabilised in the long term to 80°C.

4.2.11.2 Assessment

502 The design basis analysis presented in the PCSR (Ref. 12) and its supporting references (Refs 76 and 77) 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.

503 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.

504 It is noted that the PCSR (Ref. 12) and one of the supporting references (Ref. 77) state that the results presented for these faults are only preliminary and could be revaluated after the design is finalised. EDF and AREVA stated during GDA Step 4 through a TQ-EPR-552 (Ref. 9) that the only significant revisions to the design and analysis will be a change to the electrical supply to the FPCS and a change to the decay heat values because of the move to a single zone fuel pool. Only the preliminary analysis has been reviewed in GDA Step 4.

505 In Ref. 77, the FPCS trains 1 and 3 are identified as being supplied from Electrical Division 1. EDF and AREVA have stated that Train 1 is now to be supplied from Division 2 while Train 3 is still supplied from Division 1. An early design of the spent fuel pool considered fuel arranged in two zones of storage racks with a maximum storage capacity of 1056 assemblies. This assumption has been utilised in all the assessed calculations of decay heat assumed for spent fuel pool faults. The GDA design submitted

by EDF and AREVA is for a single zone with a capacity of up to 1167 assemblies. The change to electrical design is expected to have a beneficial effect on safety, while the change to the fuel storage zones will slightly increase the assumed decay heat but not by a significant amount (Ref. 78).

506 I was satisfied during my assessment that neither of these changes would invalidate the methodology applied nor significantly impact the safety analysis in Ref. 12, demonstrating that safety criteria have been met. This has subsequently been demonstrated in the March 2011 revision of the PCSR (Ref. 14) which incorporates the identified changes and has removed caveats on the preliminary status of the analysis. While I have not assessed the updated spent fuel pool fault analyses summarised in Ref. 14 in detail, I am satisfied that EDF and AREVA have incorporated the changes appropriately and the safety case claims and arguments continue to be supported.

507 EDF and AREVA's design rules for PCC events require Class 1 (F1A) systems to achieve the controlled state and a minimum of Class 2 (F1B) systems to go from the controlled state to the safe shutdown state. Chapter 14.0 of the PCSR (Ref. 12) provides a special definition of the controlled state for the spent fuel pool, differentiated from the general definition applied to reactors. It is characterised by the short term removal of decay heat. For faults involving a loss of a FPCS cooling train, given the long time before possible fuel exposure (several hours even in the most limiting scenarios), it is assumed that the controlled state is reached at the start of the transient. For fuel pool draining faults, the controlled state corresponds to a water inventory that is stabilised by stopping the draining without any fuel being uncovered. The safe state is characterised by the permanent removal of decay heat from the fuel stored in the pool by at least one FPCS cooling train, with the water temperature below 80°C. As a result of these rules, as they only have to provide a Category B function, the main FPCS trains have a safety classification of Class 2 (F1B). SSCs which are claimed to stop draining are assigned a safety classification of Class 1 (F1A).

508 While I accept that there is logic and consistency in the approach to categorisation and classification adopted by EDF and AREVA, I am not currently convinced that it is acceptable for the spent fuel pool to have no Class 1 cooling system. Refs 23 and 76 set out the design requirements for the FPCS. The piping and heat exchangers are built to class M2 (the highest standard that is applied to SSCs not part of the reactor coolant pressure boundary or in the HIC envelope). The main cooling trains are also to be built to the highest seismic and electrical standards. Therefore, many aspects of the design would be unaltered by reclassification. The one identified shortfall is C&I where there are identifiable differences in requirements between Class 1 and Class 2 SSCs.

509 Action 5 of GDA Issue **GI-UKEPR-CC-01** places a requirement on EDF and AREVA to review the safety classification of Class 3 SSCs providing a diverse means of protection for frequent faults and to demonstrate whether it is ALARP for these SSCs to be reclassified as Class 2. I have added Action 7 to this GDA Issue for EDF and AREVA to review the safety classification of Class 2 SSCs claimed to cool the spent fuel pool and to demonstrate whether it is ALARP for these SSCs to be reclassified as Class 1.

510 EDF and AREVA do consider single failures and preventative maintenance in accordance with the PCSR's stated rules for PCC design basis faults. EDF and AREVA have therefore provided the information to allow an assessment against SAPs FA.6, EDR.2 and EDR.4. The vulnerability of the design to a loss of the second main FPCS train during refuelling due to a heat exchanger failing (i.e. a single failure) following an initial loss of the other main FPCS train is argued to be acceptable because the second train is in operation before the event and remains operational with no change in state required.

In response to Action 2 of RO-UKEPR-41 (Ref. 10), EDF and AREVA have considered passive single failures associated with the main FPCS and have concluded that all safety criteria are met if the third FPCS train is claimed (in the PCSR it is only claimed for the RRC-A event). They acknowledge that their own general rules specify that PCC events must only claim F1 systems (Class 1 and Class 2) and the third train is F2 (Class 3). However, due to the specific nature of the spent fuel pool, the high thermal inertia and the low pressures, they argue that an exception can be made. They state in the RO response (Ref. 21) that the safety benefit provided by the third FPCS train is more relevant than whether it is classified as Class 2 or Class 3. I accept this argument.

511 EDF and AREVA have analysis which demonstrates the capability of the third cooling train to cool the spent fuel pool for the RRC-A event. According to EDF and AREVA's own design rules, the level of uncertainty assumed for spent fuel decay heat can be relaxed for a RRC-A fault compared to that for a PCC event. I found conflicting statements in the PCSR (Ref. 12) and Ref. 76 as to whether uncertainties had been included in the assumed decay heat loading in the pool (Chapter 9 of Ref. 12 and Ref. 76 state that the assumed decay heat is conservative, Chapter 16 of Ref. 12 states that the decay heat is best estimate). To satisfy expectations in the UK for tolerability to passive failures, it could be necessary to claim the third train of cooling for PCC events, with cooling capability demonstrated with conservative calculations. I have therefore raised an Assessment Finding, **AF-UKEPR-FS-23**, for capability of third train to cool the spent fuel pool to be definitively demonstrated on a conservative basis for the finalised UK EPR design. Despite the changes to the storage capacity and the confusion over whether uncertainties have been included in the available analysis, I do not expect a design change to be required to the third train capability because the preliminary analysis assumed out of scope MOX fuel which has a higher decay heat than the equivalent UO_2 fuel.

512 Despite the lack of this small piece of definitive evidence and the lack of a Class 1 safety classification, I am generally satisfied that the design of the cooling trains, including the diversity provided by the third train, is in accordance with SAP EDR.2. It is noted that although the UCWS and ESWS are independent systems, they both eventually give up their heat to the sea. The detailed design of the forebay configuration will be site specific although the PCSR does discuss the ability to cross-connect outflows and inlets to provide additional flexibility and defence in depth. This has been discussed further in Ref. 64.

513 The safety case for the isolatable piping failures on systems connected to the spent fuel pool (PCC-3 events in all reactor operating states) makes significant claims on anti-siphon devices to restrict the drain down level. The failure of a siphon breaker to limit the drain down level is regarded to be a passive failure and is not considered for any PCC or RRC-A event. In response to a TQ-EPR-572 (Ref. 9), EDF and AREVA have stated that a leak from a siphon breaker pipe itself will not result in the loss of its function. Siphon breakers on discharge lines take the form of J-tube shapes beneath the normal operating water level. They claim that blockage of the opening of the siphon breaker by a sucked-in piece of debris in the fuel pool is extremely unlikely because there is very little negative pressure. On the suction line, the opening of the siphon breaker is above water so there is no risk of blockage from a loose part in the water. For the latter, EDF and AREVA have commented that they would implement some means of protection against falling material. They have also suggested that there will be an extensive visual inspection of the siphon breakers during commissioning to check their operability.

514 The siphon breaker designs are simple and intrinsically reliable. Therefore I accept the arguments presented. However, the siphon breakers on the discharge lines are likely to be submerged throughout the operating life of the spent fuel pool and it is unclear if there will be periodic testing of their function during that time. Their failure to limit the drain down level has the potential to lead to fuel in-transit to be uncovered following the identified PCC-3 event and therefore it is important that they work when required. In fact, there are unclaimed check valves on the discharge lines to provide additional defence-in-depth for drain down faults. However an Assessment Finding, **AF-UKEPR-FS-24**, is made for a future licensee to identify during site licensing what checks will be made during commissioning and during the lifetime of the spent fuel pool to demonstrate that the siphon breakers are still functional.

515 No break preclusion arguments for sections of pipe are presented in the Fault Studies sections of the PCSR and its supporting references, aside from the very brief note in Chapter 14.4 of the PCSR that breaks located upstream of the isolation valves are not considered. Much stronger emphasis is made in the PCSR on the claim that the FPPS / FPCS design is 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. No vulnerability to passive failures was identified in the response to RO-UKEPR-41 (Ref. 21). However, Ref. 89 states that leaks from the following need to be excluded (by evoking break preclusion arguments) because the flow rate cannot be compensated for by normal makeup systems:

- the three FPCS suction lines from the spent fuel pool to the second isolation valve;
- the FPPS suction lines from the fuel transfer canal and the cask loading pit up to the second isolation valve;
- the FPPS suction lines from the reactor vessel pit, the reactor internals storage pit, and the fuel transfer canal of the reactor building to the second isolation valve; and
- the fuel transfer canal of the reactor building and the fuel transfer canal of the fuel building.

516 The rigour required to show that the likelihood of failure is so low that the consequences of failure can be discounted is high in UK and should not be put forward to avoid making a consequences analysis. As discussed above, the FPCS piping is currently assigned a M2 classification which represents a high nuclear standard but is not sufficient for the HIC envelope. Isolation valves do need to be placed in a practical location and inevitably some piping will be upstream of them and therefore non-isolatable. However, EDF and AREVA have not discussed how they have optimised the elevation and location of the valves to minimise the length of piping for which they need to make break preclusion arguments. As a result, I require EDF and AREVA to provide a more detailed design basis safety case for these spent fuel pool leaks previously not considered because of break preclusion arguments. This should include consequences analysis for the identified leaks and ALARP arguments to justify the current design. This requirement is captured as Action 3 of GDA Issue **GI-UKEPR-FS-03**.

517 EDF and AREVA have identified a long term loss of offsite power during normal reactor power as a PCC-3 event. i.e. a frequency between 10^{-4} per year and 10^{-2} per year. I am not convinced that long term loss of offsite power is as infrequent as this. Significantly, grid reliability is not necessarily a parameter under the control of the nuclear power plant operator and is in part independent of the level of engineering adopted in the UK EPR design. Therefore I have raised an Assessment Finding, **AF-UKEPR-FS-25**, for the future licensee to review the frequency attributed to all loss of offsite power events in the

UK (both a short and long term, and not just spent fuel pool faults) and to revise the safety criteria / mission requirements accordingly if the currently assumed frequencies cannot be supported.

518 During the assessment of the UK EPR spent fuel pool safety case in GDA Step 4, it became apparent that faults associated with the cask loading pit and the despatch of fuel from the spent fuel pool had not been considered in the PCSR (either deterministically or in the PSA). The cask loading pit is contiguous to the main pool area but is usually isolated by a hinged, permanent water-tight door and sometimes further isolated by a mobile stop-gate. However, to remove spent fuel from the pool, these doors and gates are opened. Fuel is despatched through a penetration in the bottom of cask loading pit into a "docked" spent fuel cask. This operation and the installed systems which facilitate it have the potential to cause faults which are a threat to either the spent fuel in the storage racks or to an individual fuel assembly being handled.

519 Subsequent interactions with EDF and AREVA (including a visit to Chooz B NPP in France which has a similar spent fuel pool design to that proposed for the UK EPR) established that the design of the cask loading pit and the management of despatching spent fuel off-site is a mature process that builds upon experience in France. Evidence has been provided to show that thought has been put into the design of the cask loading pit to guard against potential faults, including preventative, defence in depth measures and mitigation features.

520 From what I have seen, it should be possible for EDF and AREVA to make an acceptable safety case for their cask loading pit design, including the active despatch of fuel through a penetration in its base. However, this safety case needs to be written and provided to HSE ND for assessment. This is therefore a GDA Issue (**GI-UKEPR-FS-03**, Actions 1 and 2). Both design basis analysis and probabilistic safety analysis is to be provided.

521 The boundaries of cask loading pit safety case to be provided for GDA are limited to the time when the spent fuel cask is attached to the penetration in the cask loading pit base. The movement of loaded casks around the site and the specific design of the spent fuel casks are not necessarily fixed with the generic reactor design and therefore an end-to-end fuel route safety case is not required at this stage. However, the proposal to despatch fuel through the base of the cask loading pit is a significant aspect of the generic UK EPR design and it needs to be shown to be acceptable.

4.2.11.3 Findings

522 I am generally satisfied with the design basis safety case presented for the spent fuel pool. It is my judgement that the expectations set out in SAPs FA.4 to FA.7 are met by the analysis presented in the PCSR and supporting references. No sophisticated computer codes are used in the analysis so assessment against SAPs FA.17 to FA.24 is straightforward.

523 I require the capability of the third cooling train to cool the spent fuel pool to be demonstrated on a conservative basis. However, there are conflicting statements both within the PCSR (Ref. 12) and in its supporting references as to whether the provided analysis is conservative. This is to be resolved through the Assessment Finding **AF-UKEPR-FS-23**. I expect this Assessment Finding to be straightforward to resolve, along with the second Assessment Finding, **AF-UKEPR-FS-24**, to identify checks on the functionality of the siphon breakers.

524 The presented safety case does not consider faults associated with fuel despatch and the cask loading pit. This requirement to provide both a deterministic and probabilistic safety case for assessment against SAPs FA.1 to FA.14 has resulted in Actions 1 and 2 of GDA Issue **GI-UKEPR-FS-03**.

525 EDF and AREVA are required to provide a more detailed safety case and a consequences analysis for spent fuel pool leaks previously not considered within the design basis because of break preclusion arguments. This additional requirement is Action 3 of GDA Issue **GI-UKEPR-FS-03**.

526 I am not satisfied that the frequency of a total loss of offsite power is as low as EDF and AREVA assume. Therefore **AF-UKEPR-FS-25** has been raised for a future licensee to review the frequency assumed for a loss of grid in the UK and update the safety case accordingly.

4.2.12 Shutdown Faults

4.2.12.1 Summary of EDF and AREVA's Safety Case

527 The design basis analysis of shutdown faults is considered in the PCSR together with 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 not discussed in this section.

528 Six reactor states, A to F are clearly defined and the faults associated with the appropriate state. During State C, decay heat removal of the RCS is switched from the SGs to the LHSI pumps, operating in RHRS mode (as opposed to SIS mode). 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 reactor pressure vessel head with nitrogen before opening to atmosphere. The ¾ loop operation also allows the SGs and the RCPs to be maintained although the safety case for these activities is beyond the scope of GDA.

529 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.

530 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.

531 In States C and D, 3 SIS / RHRS trains are in operation to remove residual heat. The PCSR (Ref.12) states that 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 SI on low RCS loop level. This last signal to start MHSI is Class 1 (F1A) classified.

532 When questioned further through TQ-EPR-575 and TQ-EPR-306 (Ref. 9), EDF and AREVA stated that the SI signal on low RCS loop level not only initiates MHSI but it also isolates the RCS boundaries, including the let down line. This isolation is also Class 1.

533 Chapter 14.3 of the PCSR (Ref. 12) 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 a second train.

534 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 RPS 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.

535 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, Ref. 12), EDF and AREVA claim 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.

536 The PCSR identifies one PCC-3 shutdown fault 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 RPS and are Class 1 (F1A). As a result of this design feature, the PCSR does not consider the potential PCC-3 shutdown fault further.

537 The long term (between 2 and 24 hours) loss of off-site power in State C fault is classified in the PCSR as a PCC-4 design basis event. 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 SSS. 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.

538 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.

539 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.

540 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.

541 The PCSR presents design basis analysis for an isolatable SIS 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 Class 1 (F1A) measurements for breaks outside of the containment, allowing the SIS / RHRS to be isolated by an automatic Class 1 (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.

4.2.12.2 Assessment

542 As with at-power faults, I have assessed the design basis safety case shutdown faults against SAPs FA.4 to FA.7. In addition, the expectations for redundancy and tolerance to common cause failure set out in EDR.2 and EDR.3 still apply.

543 The design basis safety case for the uncontrolled RCS level drop fault in States C and D presented in the assessed PCSR (Ref. 12) is not fully consistent with answers provided in response to TQs. Chapter 14.3 of the PCSR discusses operational alarms and interlocks and the Class 1 (F1A) MHSI injection. However, it does not mention the Class 1 isolation of the letdown line also prompted by the safety injection signal. EDF and AREVA have indicated that it is the Class 1 isolation of the letdown line that is the principal safety claim for the design basis safety case and there are no claims made on the operational alarms and interlocks described in the PCSR. The latest version of the PCSR (Ref. 14) has been updated to reflect the revised position established via the TQ responses.

544 It should be noted that the PCSR (Ref. 12) assumes that a failure of a letdown line bounds a small break in the depressurised RCS. Isolating the letdown line will not provide any protection against the small break fault. As a result, EDF and AREVA have removed any claims of the small breaks to be bounded by the letdown fault from the revised PCSR (Ref. 14). Small breaks in shutdown states C and D are covered as an identified PCC-4 event in Chapter 14.5 of the PCSR (both Ref.12 and 14).

545 The provision of a back-up low level protection signal as a result of RRC-A PSA analysis is welcomed. These sensors are diverse to the main safety level sensor, and provide inputs to the SAS system which is independent of the main RPS protection system. It is acceptable according to SAP ECS.2 for the back-up level protection to be a lower classification to the principal means of protection. It is noted that the same SSCs are actuated by both the main safety signal and the back-up protection signal, so the RRC-A provision is not a truly diverse system. However, both the Class 1 (F1A) isolation and safety injections functions would need to fail for the uncontrolled level drop to continue. TQ-EPR-575 (Ref. 9) states that in the event of a common cause failure of the MHSI, the

LHSI pumps could be tripped from their RHRS role and restarted manually in SIS mode. Assuming the letdown line isolation has worked (with only 9 to 10 minutes before suction condition limits are met, there is insufficient time for an operator action to be claimed if the isolation has failed), then there is additional defence in depth to recover this fault.

546 I am generally satisfied with EDF and AREVA's safety case for this fault as presented in the TQ responses. The revised PCSR (Ref. 14) has confirmed that the position set out in these responses is now the formal safety case. As part of my review of EDF and AREVA's response to Action 9 in GDA Issue **GI-UKEPR-FS-02** to demonstrate diverse means of achieving the safe shutdown state from the controlled state for frequent faults, I will be looking for improved presentation and clarity of the claims for diversity.

547 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.

548 I have chosen not to assess in detail the RCCA bank withdrawal fault in shutdown states (equivalent faults during power operations have been discussed in Section 4.2.6). It is for my C&I colleagues to assess the ability of the protection system to deliver Class 1 protection systems. Assuming they have no concerns, cutting the power supply should be an adequate measure to prevent this fault occurring and removing the need for consequences analysis to be presented and assessed.

549 The tolerance of the UK EPR design to a long-term loss of off-site power during State C appears to be adequately demonstrated. 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.

550 The definition of long-term is between 2 and 24 hour. I established via TQ-EPR-573 (Ref. 9) that the time duration of 24 hours is arbitrary but EDF and AREVA state that this is based on usual practice and they consider it suitable for the design stage (which I agree with). The safe shutdown state following the fault is achieved before 24 hours with the aid of safety systems running on the EDGs. Each EDG is designed to run at full load for 72 hours, a time period that can be extended if the fuel tanks to the EDG are refilled. It would be helpful if the PCSR stated that no specific actions are claimed to terminate the fault at 24 hours (e.g. the grid returns in that time) or that no additional actions are required to extend the safe operation of the reactor beyond 24 hours (e.g. the supply of more fuel to the EDG within 24 hours). However, I am satisfied for the purposes of GDA with the overall tolerance of the UK EPR design to a long-term loss of off-site power during State C. As stated in Section 4.2.11, I am not convinced that the frequency of a long term loss of off-site power is as low as EDF and AREVA claim. Therefore, **AF-UKEPR-FS-25** has been raised requiring the future licensee to review the frequency attributed to all loss of offsite power events in the UK and to revise the safety criteria / mission requirements accordingly if the currently assumed frequencies cannot be supported. For this particular fault, it is possible that re-classification from a PCC-4 event will not change the requirements or mission times of the claimed mitigating systems.

551 The PCSR is clear about what is assumed in design basis analysis for a SBLOCA in reactor States C and D with respect to initial conditions, assumed availabilities, choice of single failures, etc. However, it does not present any specific transient analysis for the UK EPR. Instead it refers out to Flamanville 3 analysis undertaken in 2003 for the Preliminary Safety Analysis Report. This analysis has not been reviewed but it is noted

that it was performed for a 4250 MWth reactor and used CATHARE V1.3L (i.e. not the latest version, CATHARE V2.5 that has been assessed in Section 4.2.8.9).

552 While I consider the claims and arguments presented in the PCSR for this fault sufficient for GDA, I have raised an Assessment Finding for this analysis to be repeated for UK EPR specific conditions to confirm the assertions made (**AF-UKEPR-FS-26**).

553 The PCSR is similarly clear for isolatable safety injection breaks about what is assumed in design basis analysis with respect to initial conditions, assumed availabilities, choice of single failures, etc. However, again there is no specific analysis presented for PCC-4 events. Instead, PCSR extrapolates from available studies, none of which are for the UK EPR and some are not specific for the faults in question. The analysis, which is referenced but not presented in the PCSR, has not been reviewed.

554 An Assessment Finding has been raised for UK EPR transient analysis to be undertaken and presented in a future safety report to support the claims made for PCC-4 isolatable safety injection line break faults (**AF-UKEPR-FS-27**).

4.2.12.3 Findings

555 I am generally satisfied with the safety case presented for shutdown faults. It is integrated in the PCSR alongside at-power faults and actively considers single failures, etc. The design does appear to have diverse systems to protect against frequent faults. As such, there is no reason why it cannot be assessed against the requirements of SAPs FA.4 to FA.7.

556 For me to be fully satisfied, I require additional evidence in the form of UK EPR transient analysis of SBLOCA and isolatable safety injection line break faults to be provided. As a result, I have raised Assessment Findings **AF-UKEPR-FS-26** and **AF-UKEPR-FS-27**.

557 As identified in my assessment of the spent fuel pool safety case, I am not satisfied that the frequency of a total loss of offsite power is as low as EDF and AREVA assume. Therefore **AF-UKEPR-FS-25** has been raised for a future licensee to review the frequency assumed for a loss of grid in the UK and update the safety case accordingly.

4.2.13 Heterogeneous Boron Dilution Faults

4.2.13.1 Summary of EDF and AREVA's Safety Case

558 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.

559 Heterogeneous boron dilution faults are not considered explicitly amongst the design basis faults discussed in Chapter 14 of the PCSR (Ref. 12). 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.

560 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 Class 1 (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.

561 The maximum possible slug is claimed to be 4 m^3, which corresponds to the total volume of the U-leg piping between the SG and RCP.

562 Analysis undertaken with the CFD code STAR-CD has been reported (Ref. 79). 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 slug size' for PSA assessment.

563 The PSA analysis (Ref. 80) calculated the probability of scenarios leading to a slug larger than 4 m^3 to be 5.2 x 10^{-9} per reactor year. On that basis, fast reactivity accidents as a result of heterogeneous boron dilution are argued to be practically eliminated.

4.2.13.2 Assessment

564 The limited analysis presented in Chapter 16.3 of the PCSR (Ref. 12) was assessed in GDA Step 3. This resulted in a RO-UKEPR-65 (Ref. 10) being written requiring EDF and AREVA to present the aspects of their heterogeneous safety case that had been developed and to set out their intentions to close the gaps in the safety case. Ultimately the RO required them to provide a complete safety case for heterogeneous boron dilution for assessment by HSE ND in GDA Step 4.

565 It was established that the analysis available at the start of GDA Step 4 was about 10 years old. EDF and AREVA already had a programme in place to revise this analysis, using an updated CFD model and incorporating design changes made since the original analysis for externally initiated faults was developed. In addition, the programme anticipated the requirement of the RO to close the gap in the safety case for intrinsic dilutions related to certain fault conditions.

566 EDF and AREVA were unable to complete this analysis programme in time for assessment by HSE ND in GDA Step 4. As a result, the actions within RO-UKEPR-65 have not been completed and it has not been possible to reach a conclusion on the adequacy of the RP's safety case. The requirement for EDF and AREVA to provide an acceptable safety in this technically complex area, originally set out in RO-UKEPR-65, remains in form of a GDA Issue (**GI-UKEPR-FS-01**).

567 Arguments that heterogeneous boron dilution faults are practically eliminated and do not need a full design basis analysis treatment due to probabilistic arguments taking benefit for engineered safety measures are unlikely to be accepted.

568 CFD analysis is a developing methodology, which offers insights into complex scenarios like heterogeneous boron dilution faults. However it can be sensitive to many variables, for example the skill of the practitioner, fine details of the model, the assumed boundary conditions, etc. Validation of the CFD model is both important and difficult. HSE ND

therefore encourages EDF and AREVA not to provide a safety case heavily reliant on claims derived directly from CFD analysis.

569 From preliminary information provided to HSE ND, EDF and AREVA are claiming that the size of any unborated slug of water will be limited by safety classified boron meters. EDF and AREVA need to provide evidence that these devices are capable of delivering this function to the requisite reliability.

570 For those faults where the size of an unborated slug is restricted by other means, for example following a SG tube plugging error, EDF and AREVA also need to provide evidence they too are capable of delivering this function to the requisite reliability. A heavy reliance on administrative controls is likely to be subject to scrutiny by HSE ND.

571 HSE ND commissioned GRS to undertake confirmatory analysis of both externally and intrinsically generated unborated slugs of water (Ref. 81). Using boundary conditions identified in the *old* analysis and available AREVA drawings of the UK EPR reactor vessel, GRS has developed an otherwise independent CFD model for analysis purposes, using a different CFD package and allowing the experienced analyst to make their own judgements on the best way to model the fault. When applied to the assessment of an externally originating slug of water, the general trends with respect to mixing with borated water in the reactor vessel are similar to those predicted by EDF and AREVA. However, the key parameter of boron concentration at the inlet of reactor core is predicted to be significantly worse (i.e. the slug is less well mixed). While EDF and AREVA have defended their analysis as being more appropriate, the confirmatory analysis does illustrate the sensitivity of CFD to changes in key parameters. As stated above, EDF and AREVA will be required to provide additional validation evidence to support their CFD analysis and/or alternative safety case arguments which increase robustness of the totality of the safety case.

572 AREVA have for a number of years conducted valuable experiments on PWR thermal-hydraulics at their PKL facility in Germany. Some of these were carried out through an OECD international framework which both HSE and GRS were participants. Amongst the phenomena investigated was reflux-condensation following a SBLOCA. EDF and AREVA have indicated that these experiments are informing their assessment of the intrinsic faults and are providing a source for boundary conditions in analysis.

573 The majority of the reflux condensation experiments were designed to address faults on the German Konvoi PWRs. The geometry of the primary circuit of the UK EPR and Konvoi reactors is similar (the original EPR design built upon the experience gained with the Konvoi reactors). However the U-leg between the SG and RCP where an unborated slug can form is slightly smaller in the UK EPR and there are significant changes in the safety injection systems and secondary side cooling scenarios. GRS's advice to HSE, supported by transient analysis undertaken with their ATHLET code, is that the capability of condensation and accumulation of an unborated slug in the U-leg is significantly smaller for the UK EPR than the Konvoi plants which prompted the international experiments at PKL.

574 While this suggests that the UK EPR is less susceptible than earlier PWRs to intrinsic heterogeneous faults, EDF and AREVA still need to provide an adequate safety case for these faults. This has not been done in GDA Step 4 of GDA, and therefore the GDA Issue **GI-UKEPR-FS-01** has been raised.

4.2.13.3 Findings

575 EDF and AREVA have not provided a comprehensive response to RO-UKEPR-65 during GDA Step 4. As a result it has not been possible to assess EDF and AREVA's safety case in this area further. GDA Issue **GI-UKEPR-FS-01** has been raised requiring the RP to provide such a safety case for assessment.

4.2.14 Internal Hazards

576 Faults in this category are caused by on-site hazards that have the potential to result in the loss of essential support systems on the reactor. These faults include fire, internal flooding, steam release from pressure systems, drop loads, missiles and hydrogen explosions. From the perspective of transient analysis, faults in this category are generally bounded under the consequences of the fault and presented in the previous sections.

577 The aim of EDF and AREVA is to ensure that internal hazards do not prevent F1 functions being fulfilled or trigger PCC-3 or PCC-4 events or jeopardise the divisional separation of safety trains. In particular, they intend to ensure an internal hazard does not adversely effect more than one element of a set of redundant F1 systems or affect the stability/integrity of the reactor coolant pressure boundary, reactor internals including fuel, secondary side pressure boundary, fuel pool including fuel, safety classified buildings, fire barriers and break preclusion pipework.

578 Unfortunately, Chapter 13.2 of the PCSR does not present any substantiation of how the high level principles discussed above have been met in practice by the design. However, HSE ND has been provided with the safety requirements document for defining the safeguard auxiliary and electrical building fire zones (Ref. 82) as an example of how these principles will be met in practice. The detail assessment of this document is presented in the Internal Hazards Assessment Report (Ref. 83) and is not discussed in any detail in this report. Nevertheless, it has been reviewed from a Fault Studies perspective as it provides an indication of how the interface between internal hazards and Fault Studies has been handled by EDF and AREVA.

579 Two sets of safety analyses are presented in Ref. 82. The first is to define the requirements to ensure that a fire cannot aggravate a PCC fault in a more onerous way than the single failure already assumed in the PCC analysis (i.e. that no more than one train of an F1 system is located in any one fire zone). It concludes that this requirement is met with the exception of the fuel pool, the F1 cooling equipment for which is only contained within two divisions. It is argued that in this case the F2 train is available for cooling unless there is additional preventative maintenance work in which case operator action is claimed for recovery.

580 The second analysis is to review each of the PCC-2, 3 and 4 events to see whether there is potential for any of them to be caused by a fire in any of the safeguard auxiliary buildings or the electrical buildings and also cause an additional failure in a system more onerous than the assumed single failure. The systems reviewed are the start-up of the EFWS, MHSI, LHSI, RHRS, MSRT, EBS and isolation of the MFWS, MSSS, accumulators, CVCS letdown and charging, PSV opening/closing and RCP tripping. The essential argument is that most systems are four fold redundant and therefore providing the fire only initiates the PCC fault together with the failure of single train, then the remaining three trains can still perform the safety function after accounting for a single failure and a train being out for preventative maintenance. As noted in Section 4.2.3.3, the EFWS is really only a 2-out-of-4 system but the operator can trip the RCPs, realign

the feed system, or perform a bleed and feed operation to overcome the single failure. There are exceptions. There are some two fold redundant systems (CVCS isolation valves, EBS trains and spent fuel pool cooling trains) but these are provided with diverse systems (containment isolation, CVCS charging, and a third spent fuel pool cooling train) that can provide the safety function, or where the safety function is only needed for transition to the safe shutdown state and where long timescales and alternative strategies are available (accumulator isolation, manual PSV operation). This information needs to be captured within the PCSR and the Fault Schedule and extended to cover fire zones in other buildings containing important safety systems to ensure that the safety barriers are appropriately classified. For this reason, Action 3 of the cross-cutting GDA Issue, **GI-UKEPR-CC-01**, requires EDF and AREVA to incorporate internal hazards into the Fault Schedule (or an equivalent format to be agreed with HSE ND).

4.2.15 External Hazards

581 Faults in this category are caused by off-site hazards that have the potential to result in the loss of essential support systems on the reactor. These faults include natural hazards such as seismic events and external flooding. From the perspective of transient analysis, faults in this category are generally bounded under the consequences of the faults presented in the previous sections.

582 The assessment of external hazards is reported separately since it has its own technical topic area (Ref. 84). External hazards are therefore not discussed in any detail in this report. Nevertheless, the area has been briefly reviewed from a Fault Studies perspective as it provides an indication of how the interface between external hazards and Fault Studies has been handled by EDF and AREVA.

583 The aim of EDF and AREVA is to ensure that consequences of external hazards are controlled and limited to ensure that the safety functions performed by structures, systems and components required to bring the plant to the safe shutdown state are not affected by the hazard and that design provisions are made to protect structures, systems and components against the effects of a consequential internal hazard.

584 Unfortunately, Chapter 13.1 of the PCSR (Ref. 12) does not present any substantiation of how the high level principles discussed above have been met in practice by the design. No functional analysis is presented to justify which safety systems are required to reach the safe shutdown state for each external hazard. Furthermore, external hazards are not presented within the Fault Schedule, so it is difficult to see whether the barriers protecting against the fault are appropriately categorised and classified. For this reason, Action 3 of cross-cutting GDA Issue, **GI-UKEPR-CC-01** also includes the requirement for EDF and AREVA to incorporate external hazards into the Fault Schedule.

4.3 Radiological Consequences of Design Basis Events

585 Site specific calculations for design basis radiological consequences are out of scope of GDA. The intention of EDF and AREVA has always been to provide site specific calculations at a later date as part of nuclear site licensing. However, to gain confidence that an acceptable UK EPR site specific safety case will be possible in the future, it is necessary to know for GDA that the radiological consequences predicted for a generic site can be compared favourably with the established UK limits. For the comparison to be meaningful, any analysis methodology needs to be compatible with that assumed to derive the UK limits. For GDA, I interpret this as “broadly consistent” and some minor differences in approach from that usual seen in the UK are acceptable.

586 SAP FA.7 states that design basis analysis of fault sequences should demonstrate, so far as is reasonably practicable, that:

- none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactivity are breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;
- there is no release of radioactivity; and
- no person receives a significant dose of radiation.

587 Where releases do occur, then doses to persons should be limited. The numerical targets to be met by design basis faults are set out in Target 4 of the SAPs.

588 EDF and AREVA's general approach in the PCSR is to apply decoupling criteria to faults, such that if these criteria are met (e.g. there is always an acceptable margin to DNB, or the fuel clad temperature does not exceed an identified temperature limit) then SAP FA.7 is met for most faults implicitly.

589 In Chapter 14.6 of the PCSR (Ref. 12), EDF and AREVA have identified a "Representative List" of 13 design basis faults for which radiological consequences analyses have been undertaken.

1	Large Break Loss of coolant accident (LOCA)	PCC-4
2	Small break LOCA	PCC-3
3	Rupture of a line carrying primary coolant outside containment	PCC-3
4	Failure in liquid or gaseous waste system	PCC-3
5	Failure of an equipment containing radioactivity in Nuclear Auxiliary Building	PCC-4
6	Steam generator Tube Rupture of 1 tube	PCC-3
7	Steam generator Tube Rupture of 2 tubes	PCC-4
8	Fuel Handling accident	PCC-4
9	Long-term Loss of offsite Power	PCC-3
10	Main Steam System Depressurisation	PCC-2
11	Loss of condenser vacuum	PCC-2
12	Multiple failure of systems in Nuclear Auxiliary Building under earthquake boundary conditions	Equivalent to PCC-4
13	RHRS failure outside containment	PCC-4

590 EDF and AREVA claim that each PCC event can be linked and bounded by at least one of the representative faults. In addition, the Representative List covers the various locations of possible leakage on site such as containment, safeguard building and fuel building etc.

591 The "headline" radiological consequences analysis presented in Chapter 14.6 of PCSR (Ref. 12) makes assumptions established during the Basic Design Phase of the EPR project and are partly based on German regulations. To provide additional information to

the French regulator, the PCSR also presents a limited number of calculations utilising assumptions consistent with those used by EDF in the assessment of the radiological consequences in their French fleet.

592 I commissioned Serco to review the submitted radiological consequences analysis against the requirements of the SAPs and the relevant Technical Assessment Guide (Ref. 85). A significant area of focus was the degree of conservatism in the "German" and "French" calculations and how the results generated compare with HSE SAPs Target 4 for off-site public releases. Serco's findings are presented in Ref. 86.

593 The key conclusions of Serco's review are:

- The PCSR does not explicitly consider UK expectations. The two methodologies offered are designed for comparison against German / French targets and therefore do not lend themselves to easy comparison with Target 4. It is acknowledged that the methodologies used are widely recognised approaches in Germany and France, and have been developed to ensure compliance with the same international standards and European directives that are the foundation of the UK limits.
- The main shortfall hindering direct comparison with Target 4 arises from grouping accidents in wide PCC frequency bands (see Section 4.1.1) under bounding radiological consequences. The Fault Schedule (Ref. 24) provides more explicit frequencies but considerable interpretation remained necessary to determine if all faults are bounded by the Reference List accident consequences. This was necessary as strictly summed frequencies were necessary for direct comparison with Target 4. This is only a potential issue for consequences above 1mSv.
- The completeness of the UK EPR design basis list of faults has been commented on in Section 4.1.6 and some omissions indentified. Therefore the Reference List of faults may not be fully comprehensive. However, while the range of Reference List accidents has some recognised omissions being addressed within the wider safety case, those presented in Chapter 14.6 of the PCSR (Ref. 12) were judged to be reasonably comprehensive and sensible when compared to those PCC faults presented in the rest of Chapter 14 of the PCSR, with a clear provenance from reactor development outside the UK.
- Taking the results at face value, the SGTR, fuel handling and PCC-4 LBLOCA scenarios appear to be the most challenging accidents, particularly when including the impact of increases in dose indicated during sensitivity studies in the PCSR and could exceed Target 4. "French" dose results are generally higher than the "German" results but not always and they are generally of similar order.
- The PCSR makes reasonable efforts to identify the key parameters but a number of claims that can significantly influence the results would benefit from more robust substantiation.
- The assumptions used to derive the core / fuel inventory should prove to be reasonably conservative if they are consistent with the UK EPR fuel enrichment and operating strategy.
- Thermal analyses of some design basis faults use the DNB decoupling criteria to ensure that fuel damage should not arise but a number of the radiological consequences assessments of the same faults conservatively assume that a degree of fuel damage does occur.

- The “French” model assumes more fuel damage in fuel handling accidents than the “German” model but neither adequately justifies the claimed level of damage based on the types of accidents that could arise.
- The “French” model has prudently considered the impact of higher burn-up and MOX fuel management strategies on nuclide release rates from damaged fuel.
- Although there are some anomalies, the spiking factors used in the “French” and “German” analyses appear to be of the right order.
- There is a notable difference between the overall “German” and “French” approaches. The general premise for the “German” analyses is that a sufficiently conservative result is obtained if parameter values that have only a 5% probability of being exceeded are used, based on known measured data probability distributions. This is applied to the determination of:
    - Fission product inventory
        - in the primary coolant (based on 95% of Experience Feedback of Konvoi and N4 plants);
        - in the adjacent plant systems taking into account the specific system data (except for specific activities in the secondary system).
    - Atmospheric dispersion and deposition conditions (based on variations in measured weather data for a French coastal site).
    - Dose contributions from a limited range of nuclides such that the calculated doses can be expected to be at least 95% of the values obtained by taking all the nuclides into account.

- The “German” approach is therefore a more realistic approach, more aligned with probabilistic type approaches rather than the more deterministic UK design basis analysis approach. The “French” approach is more aligned with the UK from this viewpoint.
- There is generally a lack of visibility of the detailed application of the transport and retention parameters used to derive release activities during accidents from the fuel, primary coolant or secondary coolant activities. Nevertheless, the analyses sampled by Serco during their review provided them with reasonable confidence in the application of the claims for these processes.
- Although there are differences in dispersion parameters, in general, the “French” and “German” Gaussian based dispersion models are comparable to the UK R-91 models and should generally provide results of similar order. The dose results can, however, vary more significantly depending on the detailed parameter assumptions that go into the overall model and may require further scrutiny dependent on the details of the accident scenarios of the site licence submission.
- Overall there is reasonable confidence in the provenance of the computer codes used in Ref. 12 at the GDA stage, with the expectation of a more formalised validation suite for the site licence submission.
- On balance, the “French” analysis seems generally more appropriate to UK design basis analysis methods, but this is not always more conservative than the “German” approach in certain circumstances.

594 Through my own assessment of Chapter 14.6 of the PCSR (Ref. 12) and Serco's review (Ref. 86), I am satisfied that it should be possible for future site specific analysis of design basis faults to show compliance with Target 4 of the SAPs.

595 While new site specific calculations have always been envisaged, I have still raised an Assessment Finding for site specific design basis radiological consequences analysis to be performed, taking due cognisance of usual UK methodology assumptions and explicitly comparing the results against Target 4 (**AF-UKEPR-FS-28**). It is acceptable to continue to use assumptions derived from either the "German" or "French" methodologies but these have to be justified on a case-by-case basis as being appropriate for the UK.

596 It is recommended that any future calculations give additional consideration to single failure assumptions and the selection of sensitivity cases. Design basis analysis of PCC events generally gives due consideration of single failures to pessimise the thermal hydraulic consequences of a particular transient. However, alternative assumptions of the limiting single failure in the radiological consequences analysis could have a significant impact on this final stage of assessment. These alternative single failure assumptions may be best investigated via sensitivity studies. The PCSR identifies two specific sensitivity studies already performed for a PCC-4 LOCA fault on a generic site. One of these considers the possibility of leakage from the reactor building to a peripheral building resulting in an unfiltered discharge. The other concerns the possibility of a single passive failure (i.e. a pipe break) in a safety system 24 hours into the fault during recirculation mode. The requirement to consider these sensitivity studies was set out in the Technical Guidelines originally applied to the EPR reactor design process (Ref. 90). There is likely to be continued merit in these sensitivities which were identified by German and French experts in 2000 but it will be for the future UK licensee to identify and justify which sensitivities to consider. Thought should be given as to whether these and other potential sensitivities should be applied individually or whether it is appropriate to combine some to ensure a bounding calculation for design basis faults.

597 Hazards are not currently on the Fault Schedule or amongst the Reference List set of faults. Following the inclusion of the hazards within the design basis (GDA Issue **GI-UKEPR-CC-01**, Action 3) due consideration will need to be given to the adequacy and completeness of the list of faults for which the radiological consequences are assessed. It is noted that in response to TQ-EPR-792 (Ref. 9), EDF and AREVA have stated that there is ongoing work to meet a French Safety Requirement to verify that the radiological consequences of hazards at Flamanville 3 are enveloped by the radiological consequences of the PCC events according to their estimated frequency of occurrence.

4.4 Overall Review of the Design Basis Analysis

598 SAP FA.8 requires that design basis analysis should demonstrate that all design basis initiating events are addressed, all safety functions of design are identified, that the performance requirements for safety systems are identified and that suitable and sufficient safety systems are provided. Furthermore, SAP FA.9 requires that the design basis assessment should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function. In my judgement, based upon my assessment of the design basis analysis performed by EDF and AREVA reported above, these requirements have been met apart from those exceptions where GDA Issues have been identified.

4.5 Limits and Conditions

599 SAP FA.9 also requires that the design basis assessment should provide an input into the limits and conditions for safe operation and identify the requirement for operator actions. In particular, the design basis analysis should provide the basis for determining the safety limits for actuator trip settings and performance requirements for safety systems, the conditions governing permitted plant configurations and the availability of safety systems, the safe operating envelope defined as operator limits and conditions in the operating rules for the facility. As noted in Section 2.3.6 above, it has been agreed with EDF and AREVA that it is more appropriate to assess the proposed technical specifications during the site licensing process. However, HSE ND has required that EDF and AREVA define the process for identifying the limits and conditions that will be incorporated into the Technical Specifications. Their proposals are reported in the responses to RO-UKEPR-55 and RO-UKEPR-72 (Ref. 10). The latter covers the safety analysis bounding limits (SABL) for the core, which are assessed in the Fuel and Core Assessment Report (Ref. 15) while the response to RO-UKEPR-55 presents only high level principles in the fault analysis area. Nevertheless, the design basis analyses reported in Chapter 14 of the PCSR are quite clear in stating what assumptions are made about preventative maintenance and single failures within the analysis. In my opinion, it should be such relatively straightforward to translate this into Technical Specifications during the site licensing process.

600 In contrast, the RRC-A analysis and the work performed on diversity in RO-UKEPR-41 assume full plant availability. Given the assumption of common mode failure considered in these sequences, I believe it is not unreasonable to discount the likelihood of an additional single failure as being outside the design basis frequency limit of 1×10^{-7} per year for all but the most frequent (and therefore more benign) faults. It is less clear whether this is the case for a preventative maintenance. In practice this may not be a significant issue as many of these sequences are ATWT sequences where the SAS and NCSS systems have multiple redundancy and the PCSR is clear that preventative maintenance will not be allowed on the EBS. This issue will need to be reviewed when the Technical Specifications are being assessed but it is my judgement that they are unlikely to result in design changes. It should be noted that there is also scope for technical input from the PSA on these matters.

4.6 Support to the GDA Structural Integrity Assessment

601 As noted in my assessment plan, it was always my intention to assess the thermal hydraulic analysis undertaken in support of the Structural Integrity Assessment of the UK EPR in collaboration with my structural integrity assessment colleagues. In practice, EDF and AREVA are still in the process of carrying out a programme of fracture analysis work to justify claims on defect tolerance of key structural components and so it has not proved possible to perform this assessment during GDA Step 4. Completion of this programme of work is covered under GDA Issue **GI-UKEPR-SI-01**. My intention is to assist my structural assessment colleagues with their assessment of the response to this GDA Issue when it becomes available by performing on a sampling basis an assessment of the transient analysis work that is being performed in support of this work.

4.7 Fault Schedule

602 In response to RO-UKEPR-41, EDF and AREVA provided HSE ND with a Fault Schedule for the UK EPR (Ref. 24). This supersedes the version of the Fault Schedule presented

in Chapter 14.7 of the PCSR (Ref. 12). A cursory review of the updated version of the PCSR (Ref. 14) has established that new Fault Schedule is captured in the same Chapter, replacing the previous version.

603 I have assessed the Fault Schedule against SAP ESS.11 and have concluded that its structure and intent meet my expectations.

604 It provides a useful and concise summary of the design basis safety case for all PCC and RRC-A events. Faults are identified and referenced, frequencies attributed, and the front line SSCs claimed to provide safety functions are identified (together with their safety classification).

605 In addition to identifying the principal SSCs claimed in the design basis analysis to fulfil safety function, diverse SSCs are identified for frequent faults to provide the same safety function. It is noted the Fault Schedule only demonstrates diversity to achieve the controlled state. Ref. 24 does not attempt to demonstrate diversity to the safe shutdown state. Action 9 of GDA Issue **GI-UKEPR-FS-02** has been raised for EDF and AREVA to address this shortfall.

606 Ref. 24 appears to be an accurate representation of the UK EPR design basis safety case at the time of its issue, which is an acceptable position. The individual entries for each fault have only been sampled but those reviewed reflect the claims made in main text of the Fault Studies PCSR chapters. During GDA, I have required EDF and AREVA to justify and extend the scope of their design basis safety case. The demonstration of diversity is an example of where the Fault Schedule encompasses the expansion in the scope of EDF and AREVA's safety case. The inclusion of hazards within the design basis safety case is still being developed through a cross-cutting GDA Issue **GI-UKEPR-CC-01** and therefore these are not included on the Fault Schedule. An Assessment Finding is made for the Fault Schedule to be updated as a minimum as part of each major safety submission to HSE ND to reflect the design basis safety case at that time and contained in the submission (**AF-UKEPR-FS-29**).

607 The Fault Schedule illustrates that many of the SSCs providing diverse protection to frequent faults are the same as those claimed for equivalent RRC-A faults. In the original UK EPR design, SSCs claimed for RRC-A events must have a minimum classification of Class 3 (F2). HSE ND's expectation of the safety classification for a SSC that makes a significant contribution (but not the principal means) to fulfilling a Category A safety function is Class 2. The visibility Ref. 24 gives to the safety classification allowed HSE ND to easily identify those SSCs whose safety classification could potential fall short of expectations outlined in SAP ECS.2. EDF and AREVA are addressing this issue through the cross-cutting GDA Issue **GI-UKEPR-CC-01**. The Fault Schedule is to be updated reflect the conclusions of this GDA Issue.

4.8 Commissioning Test Programme

608 In Chapter 19 of the PCSR, EDF and AREVA have outlined their approach to developing the commissioning test programme for the UK EPR. As noted in Section 4.2.2 above, Assessment Finding **AF-UKEPR-FS-06** requires the future licensee to review the validation evidence for the MANTA code and identify whether there are any commissioning tests that can be performed upon the UK EPR to help increase confidence in the validation of these codes. Any tests that are identified will need to be factored into the commissioning programme for the first of kind reactor.

4.9 Overseas Regulatory Interface

609 HSE's Strategy for working with overseas regulators is set out in Refs 87 and 88. In accordance with this strategy, HSE collaborates with overseas regulators, both bilaterally and multinationally. In particular, ND collaborates through the work of the International Atomic Energy Agency (IAEA) and the OECD Nuclear Energy Agency (NEA) representing the UK in the Multinational Design Evaluation Programme (MDEP). The latter is a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. This helps to promote consistent nuclear safety assessment standards among different countries. There have been two MDEP meetings for the EPR in the fault analysis area.

610 HSE ND has formal information exchange arrangements to facilitate greater international co-operation with the nuclear safety regulators in a number of key countries with civil nuclear power programmes. These include:

- the US Nuclear Regulatory Commission (US NRC);
- the French L'Autorité de Sûreté Nucléaire (ASN);
- the Finnish Radiation and Nuclear Safety Authority (STUK).

611 Specifically, in the Fault Studies area, a number of meetings have been held with the US NRC to keep them informed of the fault analysis aspects of the UK EPR GDA. Following on from these discussions, the US NRC has provided access to the input decks for the TRACE and MELCOR computer codes for the purposes of performing confirmatory analysis using technical support contractors.

612 ND is also 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.

613 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.

5 CONCLUSIONS

5.1 Key Findings from the Step 4 Assessment

614 EDF and AREVA have undertaken a large amount of analysis work within the Fault Studies assessment area during GDA Step 4 and have made very significant progress against the issues identified in my GDA Step 3 Assessment Report.

615 In my opinion, EDF and AREVA have considerably strengthened the design basis safety case for the UK EPR through the additional analysis performed in response to the ROs raised in my GDA Step 3 Assessment Report. They have performed a large number of additional sensitivity studies and have demonstrated that the design is particularly well protected against passive single failures. They have also been able to extend the design basis to cover complex situations in which a combination of events may initiate a fault sequence, although this is an area where there is still some further work to be done by the RP and a GDA Issue has been raised.

616 The analytical work performed by EDF and AREVA has been aided by a number of important design changes to the C&I systems on the UK EPR that in my opinion will significantly improve the safety of the design. These changes have been proactively identified by EDF and AREVA. The design changes identified are:

- An increase in the partial cooldown rate from 100°C/hr to 250°C/hr following a loss of coolant accident. This has considerably increased the margin of safety on the clad melt temperature limits for the loss of coolant accidents that EDF and AREVA consider to be within the design basis of the UK EPR.
- Addition of a high neutron flux trip signal and a high axial offset trip signal on one of the diverse reactor protection systems to improve protection against reactivity faults occurring together with a failure of the main reactor protection system.
- Addition of a high hot leg pressure trip signal on one of the diverse reactor protection systems to improve the protection against loss of normal feedwater faults occurring together with a failure of the main reactor protection system.
- Addition of a low RCP speed trip signal on one of the diverse reactor protection systems to improve the protection against reduction in flow faults occurring together with a failure of the main reactor protection system.
- Addition of an automatic actuation signal to start the EFWS using a low SG water level signal on a diverse reactor protection system to improve protection against loss of main feedwater faults occurring together with a failure of the main reactor protection system.
- An improvement to the integrity and detection capability of the activity detectors on the secondary side steam lines to provide better protection against SGTR faults.

617 In my judgement, any additional design changes resulting from the identified GDA Issues will be limited to the C&I systems. The one exception could be **GI-UKEPR-FS-05** because the design basis assessment could result in changes to the categorisation and classification of systems that protect against the loss of essential support systems. Nevertheless, in my opinion, it is now highly unlikely that there will be a need for any significant changes to plant layout or the addition of any new safety systems to UK EPR design from a Fault Studies perspective.

618 Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK EPR reactor design. The UK EPR reactor is therefore suitable for construction in the UK, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.1.1 Assessment Findings

619 I conclude that the following Assessment Findings listed in Annex 1 should be programmed during the forward programme of this reactor as normal regulatory business.

5.1.2 GDA Issues

620 I conclude that the GDA Issues identified in this report must be satisfactorily addressed before Consent can be granted for the commencement of nuclear island safety-related construction. The complete GDA Issues and associated action(s) are fomally defined in Annex 2.

6 REFERENCES

1 *GDA Step 4 Fault Studies Assessment Plan for the EDF and AREVA UK EPR.* HSE-ND Assessment Plan AR 09/049. April 2010. TRIM Ref. 2009/455991.

2 *ND BMS. Assessment Process.* AST/001, Issue 4. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm.

3 Not used.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008.www.hse.gov.uk/nuclear/saps/saps2006.pdf.

5 Not used.

6 *Step 3 Fault Studies Assessment of the EDF and AREVA UK EPR*. HSE-ND Assessment Report AR 09/028. November 2009. TRIM Ref. 2009/335832.

7 Not used.

8 Not used.

9 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600726.

10 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600727.

11 Not used.

12 *UK EPR Pre-construction Safety Report – November 2009 Submission.* Submitted under cover of letter EPR00226N. 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

13 *UK EPR Master Submission List.* March 2011. TRIM Ref. 2011/200786.

14 *UK EPR Pre-construction Safety Report – March 2011 Submission.* Submitted under cover of letter EPR00844N. 31 March 2011. TRIM Ref. 2011/200260 and as detailed in UK EPR Master Submission List. March 2011. TRIM Ref. 2011/200786.

15 *Step 4 Fuel and Core Design Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-021. Revision 0. TRIM Ref. 2010/581511.

16 *Step 4 Fault Studies – Containment and Severe Accidents Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-020b. Revision 0. TRIM Ref. 2010/581403.

17 *Success Criteria for PSA for UK EPR*. GRS-V-HSE-WP12, 15 & 15a-01. GRS. January 2011. TRIM 2011/109457.

18 *Step 4 Probabilistic Safety Analysis of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-019. Revision 0. TRIM Ref. 2010/581512.

19 *ND BMS. Technical Assessment Guide. Transient Analysis for DBAs in Nuclear Reactors.* T/AST/034, Issue 1. November 1999. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast034.pdf.

20 *ANSI/ANS-5.1-1983. Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.* American National Standards Institute (ANSI). April 1983.

21 *Passive Single Failure Analysis*. NESS-F DC 691 Revision B. Areva. December 2010. TRIM Ref. 2011/85987.

22 *Analysis of Intermediate Breaks and Large Breaks LOCA PCC-4 Events.* NEPR-F DC 585 *Revision* C. Areva. December 2010. TRIM Ref. 2011/85981.

23 *Classification of Structures Systems and Components*. NEPS-F DC 557 Revision C. Areva. *January* 2011. TRIM Ref. 2011/85983.

24 *Faults Schedule*. PEPR-F DC 4 Revision A. Areva. June 2010. TRIM Ref. 2011/92862.

25 *Step 4 Cross-cutting Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-032. Revision 0. TRIM Ref. 2010/581499.

26 *Consistency Between PSA List and PCC List*. NEPR-F DC 584 Revision A. Areva. July 2010. TRIM Ref. 2011/92996.

27 *A preliminary report of further secondary side blow down sensitivity studies for the Sizewell B PWR.* PWR/R 772. NNC Ltd. October 1983. ID23558-1001

28 *Functional validation of the MANTA-SMART-FLICA coupling*. NEPD-F DC 10157 Revision A. Areva. October 2008. TRIM Ref. 2011/141410.

29 *EPR Methodology for steam line break analysis with the MTC 3D*. NEPR-F.DC.553 Revision A. Areva. May 2010. TRIM Ref. 2011/92995.

30 *Physical Models of MANTA Code*. NFEPD DC 50 Revision C. Framatome. January 2006. TRIM *Ref*. 2011/93004.

31 *MANTA – Code Synthetic Qualification Assessment*. NFPSD DC 85 Revision D. Areva. September 2008. TRIM Ref. 2011/141449.

32 *Qualification of MANTA code on a transient of a spurious opening of a MSRT valve on Paluel 3 Reactor. PEPR-F DC 13. August 2010. TRIM Ref. 2011/93029.*

33 *Manta Mixing Matrices for the EPR based on Juliette Tests Interpretation.* NEPD-F DC 74 Revision B. EDF and AREVA UK EPR. August 2009. TRIM Ref. 2011/92994.

34 *SCIENCE V2 Nuclear Code Package - Qualification Report.* NFPSD DC 89 Revision A. Framatome. March 2004. TRIM Ref. 2010/408510.

35 *Technical description of FLICA III F V 2.5.1 – Justification for choice of basic models*. *EPTC* DC 1470 Revision A. Framatome. February 1997. TRIM Ref. 2010/408621

36 *Qualification Report - FLICA III-F Version 3*. NFPSD DC 188 Revision A. Framatome. *January* 2006. TRIM Ref. 2010/408405.

37 *FLICA III-F V 2.5.1 Qualification Report*. EPTC DC 1469 Revision A. Framatome. February 1997. TRIM Ref. 2010/408651.

38 *Cooldown Fault Analysis for UK EPR*. GRS-V-HSE-WP17, 17a-02. GRS. March 2011. TRIM 2011/329015.

39 *Transient Analysis to Support the Generic Safety Case for Sizewell B.* C5166/TR/137. NNC. July 1998. ID381891-1001

40 *FC2002 – CHF Correlation AFA-2G-AFA-3G-FUEL*. NEPD-F DC 10306 Revision A. Areva. November 2010. TRIM Ref. 2011/85978.

41 *Main Steam Line Break.* PEPR-F DC 3 Revision A. Areva. May 2010. TRIM Ref. 2011/92861.

42 *UK EPR Reference Design Configuration.* UKEPR-I002 Revision 10. EDF and Areva. May 2011. TRIM Ref. 2011/278360.

43 *Main Steam Line Break: Break Spectra and Sensitivity Studies*. PEPR-F DC 25 Revision B. Areva. December 2010. TRIM Ref. 2011/86028.

44 Not used.

45 *Functional Diversity for Frequent Faults*. NEPR-F DC 580 Revision A. Areva. June 2010. TRIM Ref. 2011/92795.

46 *Functional Diversity for Frequent Faults Quantified Analyses*. NEPR-F DC 592 Revision A. Areva. 5 November 2010. TRIM Ref. 2011/85982.

47 *Ringhals 1 Stability Benchmark – Final Report*. Nuclear Science Committee NEA/NSC/DOC (96)22. Nuclear Energy Agency (NEA). November 1996.

48 *Sizewell B Station Safety Report*. Chapter 15. Nuclear Electric. 1992. ID507708-1001

49 *ATWS Aanalysis for UK EPR.* GRS-V-HSE-WP07-01. GRS. November 2010. TRIM Ref. 2011/46105.

50 *Refuelling* Error on Dampierre Unit-4. IRS Number 7505. International Incident Reporting System (IRS). IAEA. April 2001. TRIM Ref. 2009/407199

51 *RIA Analysis under ATWS Conditions for UK-EPR*. GRS-V-HSE-WP07a-01. GRS. January 2010. TRIM Ref. 2011/329146.

52 *Sizewell B RCCA Ejections analysis at Hot Full Power End of Cycle Conditions*. PWR/R991. NNC Ltd. March 1987. ID20721-1001

53 *EPR Sizing at 4500 MWth*. EPRR DC 1685 Revision B. Areva. July 2002. TRIM Ref. 2011/134195.

54 *Step 4 Human Factors Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment *Report* ONR-GDA-AR-11-028. Revision 0. TRIM Ref. 2010/581503

55 *Steam Generator Tube Rupture Mitigation Strategy*. PEPR-F DC 38 Revision A. Areva. December 2010. TRIM Ref. 2011/86029.

56 *Single Tube Steam Generator Tube Rupture Analysis for the UK EPR*. PEPR-F.10.1665. Areva. December 2010. TRIM Ref. 2011/86031.

57 *Multiple Steam Generator Tube Rupture (10 Tubes in One Steam Generator at Power).* NEPR-F DC 564 Revision A. Areva. February 2010. TRIM Ref. 2011/91656.

58 *Benchmark analyses against AREVA analyses for a small break LOCA and the LOOP as initiator for an ATWS*. GRS-V-HSE-WP4.4-01. GRS. October 2010. TRIM Ref. 2011/46084.

59 *Step 4 Structural Integrity Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-027. Revision 0. TRIM Ref. 2010/581504.

60 *A TRACE model of the UK-EPR*. ISL-NSAO-TR-10-15. Information Systems Laboratories (ISL). September 2010. TRIM Ref. 2010/470777.

61 *TRACE Analysis of Intermediate Break LOCAs for the UK-EPR*. ISL-NSAO-TR-10-17. *Information* Systems Laboratories (ISL). December 2010. TRIM Ref. 2011/5507.

62 Not used.

63 *M5^{TM} Properties Data (BE).* SXP-IP-813155 Revision D. Framatome. January 2005. TRIM Ref. *2010*/290468

64 *Step 4 Mechanical Engineering Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-026. Revision 0. TRIM Ref. 2010/581505.

65 *Large Break LOCA (2A) design guidelines.* TR 96/50 Revision C. Nuclear Power International. January 1997. TRIM Ref. 2010/269090.

66 *Core damage extent analysis during double-ended break LOCA for FA3 EPR reactor*. NEPD-F DC 159 Revision A. Areva. TRIM Ref. 2011/86213.

67 *Safety Significance of the Halden IFA-650 LOCA Test Results.* NEA/CSNI/R (2010) 5. Nuclear *Energy* Agency (NEA) Committee on the Safety of Nuclear Installations. November 2010. TRIM Ref. 2011/4756.

68 Not used.

69 *CATHARE 2 V2.5_1: Description of the base revision 6.1 physical laws used in the 1D, 0D and 3D modules.* SSTH-LDAS-EM-2005-038. CEA. September 2005. TRIM Ref. 2010/269058.

70 The *CATHARE* Code. DTP/SMTH/LMDS/EM/2001-063. CEA. April 2002. TRIM Ref. 2010/269015.

71 *CATHARE 2A – Break LOCA Realistic Evaluation Model*. EPTB DC 1502 Revision B. Framatome. May 1998. TRIM Ref. 2010/269096.

72 *BEMUSE Phase V Report – Uncertainty and Sensitivity Analysis of a LB-LOCA in ZION Nuclear Power Plant.* NEA/CSNI/R(2009)13. Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations. December 2009. TRIM Ref. 2010/512955.

73 *Description of the Methodology Used For the FA3 EPR to Assess the Number of Fuel Rods Failures Occurring During a 2A-LOCA Transient.* NEPD-F DC 52 Revision A. Areva. April 2007. TRIM Ref. 2010/269083.

74 *CATHARE2 V2.5_1: User Guidelines*. DER/SSTH/LDAS/EM/2005-034. CEA. February 2006. TRIM Ref. 2010/269035.

75 *CATHARE2 V2.5_1: User's Manual*. SSTH/LDAS/EM/2005-035. CEA. March 2006. TRIM Ref. 2010/269049.

76 *Plant System File PTR – Fuel Pool Cooling System Part 2 - System Operation*. SFL–EF MF 2006.712 Revision G1. Sofinel. October 2008. TRIM Ref. 2011/339515.

77 *Functional design relating to PCC treatment of loss of cooling and pool drainage.* ECEF080499 Revision A1. EDF. November 2008. TRIM Ref. 2011/86127.

78 *Residual Decay Heat Curves for Major Components Design Purposes – Heat Load Inside the Fuel Pool.* NEPC-F DC 164 Revision B. Areva. November 2008. TRIM Ref. 2011/92206.

79 *Heterogeneous Dilution: Critical Plug Size*. NGES1/2002/en/0241 Revision E. Framatome ANP. September 2004. TRIM Ref. 2010/243032.

80 *Heterogeneous Boron Dilution: PSA demonstration of dilution accident practical elimination*. NGPS4/2003/en/0120 Revision B. Framatome ANP. December 2003. TRIM Ref. 2010/243032.

81 *Unborated Slug of Water Assessment*. GRS-V-HSE-WP08-01. GRS. November 2010. TRIM Ref. 2011/143816.

82 *Safety Requirements for defining Safeguard Auxiliary and Electrical Building Fire Zones*. *ECEF070601* Revision B1. EDF. August 2009. TRIM Ref. 2011/85894.

83 *Step 4 Internal Hazards Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-017. Revision 0. TRIM Ref. 2010/581514.

84 *Step 4 Civil Engineering and External Hazards Assessment of the EDF and AREVA UK EPR™Reactor*. ONR Assessment Report ONR-GDA-AR-11-018. Revision 0. TRIM Ref. 2010/581513.

85 *ND BMS. Technical Assessment Guide. Radiological Analysis – Fault Conditions.* T/AST/045 Issue 1. June 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast045.htm.

86 *Review of Radiological Consequences from Design Basis Accidents for the UK EPR*. TCS/REGS/P1969/ND2060/OCT.10 Issue 2. Serco Commercial. October 2010. TRIM Ref. 2010/594475.

87 *New Nuclear power stations – Safety assessment in an international context*. Version 3. HSE. *March* 2009. www.hse.gov.uk/newreactors/ng05.pdf.

88 *UK Generic Design Assessment – Strategy for working with overseas regulators.* HSE. March 2009. www.hse.gov.uk/newreactors.ngn04.pdf.

89 *Exclusion of leak or break in non-isolated sections of the Fuel Pool Cooling System – Positioning of the concept and associated safety requirements.* ENSNDM100006 A. EDF. July 2010. TRIM Ref. 2011/92967.

90 *Technical Guidelines for the design and construction of the next generation of nuclear power plants with pressurised water reactors.* Adopted during the GPR/German experts plenary meetings held on October 19th and 26th 2000 (E). http://www.asn.fr/index.php/content/download/15572/100931/technical_guidelines_design_construction.pdf.

91 *UK EPR – Main Steam Isolation Valves ALARP Assessment regarding functional diversity and Single Failure Criterion*. PESS-F DC 27 Revision A. AREVA. October 2010. TRIM Ref. 2011/93037.

92 *UK EPR – Containment Isolation Valves Diversification ALARP Assessment*. PESS-F DC 28 Revision A. AREVA. November 2010. TRIM Ref. 2011/86033.

93 *GDA Issue GI-UKEPR-FS-01 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81193.

94 *GDA Issue GI-UKEPR-FS-02 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81194.

95 *GDA Issue GI-UKEPR-FS-03 Revision 2. Background and explanatory information.* TRIM Ref. 2011/81195.

96 *GDA Issue GI-UKEPR-FS-04 Revision 1. Background and explanatory information.* TRIM Ref. 2011/81196.

97 *GDA Issue GI-UKEPR-FS-05 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81197.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-01	The future licensee shall provide the validation evidence for MANTA code mixing coefficients in the lower plenum for natural circulation conditions following the tripping of the reactor coolant pumps during a main steamline break fault.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-02	The future licensee shall justify the applicability of the critical heat flux correlation used in the analysis of main steamline break faults for natural circulation conditions following the tripping of the reactor coolant pumps.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-03	The future licensee shall analyse the steamline break fault at hot zero power conditions assuming zero xenon and zero boron but with all RCCAs inserted to demonstrate that following a return to power that the fuel does not enter DNB.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-04	The future licensee shall provide the methodology for determining the uncertainty allowance for the low DNBR trip setpoint and the $DNBR_{LCO}$ site limit for Type I and Type II fault transients (as defined in Chapter 14.1 of the PCSR). This will need to include a justification of the algorithm used in the RPS for calculating these setpoints from the measurements made by the in-core detectors and the allowance for uncertainties due to the use of these detectors including the uncertainties associated with their calibration.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-05	The future licensee shall assess the radiological consequences (and demonstrate compliance with Target 4 of the SAPs) of multiple consequential steam generator tube ruptures occurring following a steamline break assuming the single failure of the Main Steamline Isolation Valve failing to close on the steamline associated with the fault.	Fuel on-site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-06	The future licensee shall review the MANTA validation report and perform a PIRT and scaling analysis to confirm the relevance of the validation evidence to the UK EPR design. and The future licensee shall perform any potential commissioning tests needed to provide further validation evidence for MANTA code identified from this review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site. Initial criticality.
AF-UKEPR-FS-07	The future licensee shall use the MANTA/SMART/FLICA coupled code to perform calculations against a NEA international benchmark such as a BWR stability benchmark (Ref. 47) or some other suitable test data agreed with the regulator.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-08	The future licensee shall gradually update the PCSR fault analysis through the licensing process such that the final safety submission accurately reflects the UK EPR design.	Fuel on-site.
AF-UKEPR-FS-09	The future licensee shall perform a quantitative ALARP assessment as to whether there should be a temporary reduction in reactor power when one EFWS pump is put into maintenance such that 1-out-of-4 EFWS pumps would provide adequate heat removal following a feedline break fault.	Fuel on-site.
AF-UKEPR-FS-10	The future licensee shall develop suitable maintenance arrangements to ensure the functional diversity of divisions 1 & 4 and divisions 2 & 3 of the Emergency Feedwater System (EFWS) pumps and the functional diversity of the emergency diesel generators and the station blackout diesel generators are ensured.	Fuel on-site
AF-UKEPR-FS-11	The future licensee shall review the feasibility of adjusting the LCO limit to avoid departure from DNB for the forced reduction in reactor coolant flow fault.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-12	The future licensee shall perform transient analysis studies to confirm that the forced reduction in coolant flow ATWT case with failure of RCCAs to insert is bounded by (or equivalent to) the loss of off-site power ATWT case with failure of the RCCAs to insert.	Fuel on-site.
AF-UKEPR-FS-13	The future licensee shall perform a sensitivity study to the loss of off-site power ATWT case with failure of the RCCAs to insert in which partial insertion of RCCAs is assumed. This is to demonstrate that the power distribution is not distorted such that fuel enters DNB.	Fuel on-site.
AF-UKEPR-FS-14	The future licensee shall justify the choice of axial off-set value that is assumed in the forced decrease of reactor coolant flow fault with an associated ATWT event and ensure that this is captured in the $DNBR_{LCO}$ limit.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-15	The future licensee shall demonstrate that for the uncontrolled RCCA bank withdrawal at power fault there is a diverse trip signal is available for the full range reactivity insertion rates and power levels.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-16	The future licensee shall demonstrate that for the uncontrolled RCCA bank withdrawal at power fault that the trip setpoints on the diverse protection system are adequate to ensure that the fuel does not enter DNB.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-17	The future licensee shall provide transient analysis to demonstrate that adequate protection is provided for a CVCS malfunction resulting in boron dilution while at power with failure of the reactor protection system to trip the reactor.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-18	The future licensee shall demonstrate that a fuel loading error involving the two most onerous fuel assemblies will not result in fuel entering DNB upon return to power.	Fuel on-site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-19	The future licensee shall provide transient analysis of PCC-3 SBLOCA faults in reactor State A (with UK EPR specific boundary conditions and assumptions) to demonstrate that all safety criteria are met, replacing what is currently presented in the GDA PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-20	The future licensee shall perform SBLOCA with ATWT sensitivity studies to investigate the margins provided by the adopted partial cooldown rate to avoid recriticality while ensuring adequate cooling of fuel.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-21	The future licensee shall provide transient analysis of the long term aspects of PCC-4 LBLOCA faults to demonstrate that all safety criteria are met, updating the CATHARE/CONPATE analysis that is currently presented in GDA PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-22	The future licensee shall ensure spurious C&I signals as initiating events are covered in the UK EPR safety case.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-23	The future licensee shall demonstrate the capability of third train of cooling to cool the spent fuel pool on a conservative basis (sufficient for it be claimed for design basis faults) for the UK EPR spent fuel pool design.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-24	The future licensee shall identify checks on the functionality of the spent fuel pool cooling siphon breakers to be undertaken during commissioning and during the lifetime of the pool.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-25	The future licensee shall review the frequency / PCC allocation attributed to all loss of offsite power events in the UK (both short and long term, reactor and spent fuel pool faults) and revise the safety criteria / mission requirements in the safety case accordingly if the currently assumed frequencies / PCC allocation cannot be supported.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Fault Studies Design Basis Faults – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-26	The future licensee shall provide transient analysis of SBLOCA faults in reactor States C and D (with UK EPR specific boundary conditions and assumptions) to demonstrate that all safety criteria are met, replacing what is currently presented in the GDA PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-27	The future licensee shall provide transient analysis of isolatable safety injection break faults in reactor States C and D (with UK EPR specific boundary conditions and assumptions) to demonstrate that all safety criteria are met, replacing what is currently presented in the GDA PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.
AF-UKEPR-FS-28	The future licensee shall provide site specific radiological consequences analysis for design basis events (including hazards), taking due cognisance of usual UK methodology assumptions and explicitly comparing the results against Target 4. Single failure assumptions and sensitivity cases should be reviewed and addressed on their merits for the UK.	Fuel on-site.
AF-UKEPR-FS-29	The Fault Schedule shall be updated as part of each major safety submission to reflect the design basis safety case at the time of the submission. The updated Fault Schedule shall be reported within in each submission.	Nuclear island safety-related concrete. Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site. Fuel on-site.

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Fault Studies - Design Basis Faults – UK EPR

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
HETEROGENEOUS BORON DILUTION SAFETY CASE
GI-UKEPR-FS-01 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Reactor Chemistry		
GDA Issue Reference	**GI-UKEPR-FS-01**	**GDA Issue Action Reference**	**GI-UKEPR-FS-01.A1**
GDA Issue	A safety case for heterogeneous boron dilution events is required. Both external dilution events and intrinsic dilution mechanisms from certain accident situations need to be addressed.		
GDA Issue Action	EDF and AREVA to provide ONR with a safety case for heterogeneous boron dilution faults. This needs to consider both external and intrinsic faults. ONR's expectation is that faults are identified as being within the design basis based on their initiating frequency and their unmitigated consequences. Arguments that heterogeneous boron dilution faults are practically eliminated and do not need a full design basis analysis treatment due to probabilistic arguments taking benefit for engineered safety measures are unlikely to be accepted. CFD analysis is a developing methodology, which offers insights into complex scenarios like heterogeneous boron dilution faults. However it can be sensitive to many variables, for example the skill of the practitioner, fine details of the model, the assumed boundary conditions etc. Validation of the CFD model is both important and difficult. ONR therefore encourages EDF and AREVA not to provide a safety case heavily reliant on claims derived directly from CFD analysis. ONR's assessment of the heterogeneous boron dilution safety case will inevitably generate questions and request further evidence. EDF and AREVA shall respond to ONR's queries on the supplied safety case and provide further evidence, especially related to: • EDF and AREVA are claiming that the size of any un-borated slug of water will be limited by safety classified boron meters. EDF and AREVA need to provide evidence that these devices are capable of delivering this function to the requisite reliability. • For those faults where the size of an un-borated slug is restricted by other means, for example following a steam generator tube plugging error, EDF and AREVA also need to provide evidence they too are capable of delivering this function to the requisite reliability. A heavy reliance on administrative controls is likely to be subject to scrutiny by ONR. • For dilution events resulting from intrinsic mechanisms, EDF and AREVA will need to provide evidence of adequate validation for any CFD derived claims used as part of a multi-legged safety case. EDF and AREVA shall update the PCSR in accordance with the agreed safety case. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A1**
GDA Issue	Demonstration of functional diversity for frequent faults		
GDA Issue Action	Implement the proposed modification to provide a diverse high hot leg pressure trip signal on an appropriately diverse protection system for a loss of normal feedwater fault with failure of the reactor protection system to trip. EDF and AREVA have identified that a modification is required to provide a reactor trip signal on high hot leg pressure on a non-TXS based protection system. This is to protect against a loss of normal feedwater fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A2**
GDA Issue Action	Provide improved protection for the excessive increase in secondary steam flow fault with failure of the reactor to trip due to either mechanical failure of the rods to insert or failure of the reactor protection system. In NEPR-F DC 592, analysis is presented for the case of excessive increase in secondary steam flow with failure of the reactor to trip. The analysis demonstrates that for such transients, the fault continues for a considerable period and that the variation in DNB is significant. This is true for both the mechanical failure of the rods to insert and the failure of the TXS-based reactor protection system: • In the case of the mechanical failure to insert, the position has been made worst by the recent design change to increase the partial cooldown rate for SBLOCA faults which has resulted in a relaxation of the SG pressure drop trip set point which now means that low SG level is the most effective trip parameter for these faults. • In the case of mechanical failure of the rods to insert, EDF and AREVA will justify why it is not ALARP to provide an additional trip signal or tighten the protection set points for this fault. • In the case of TXS failure, EDF and AREVA will perform an ALARP study to explore the feasibility of providing an extra trip parameter on a non-TXS based diverse protection system. Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A3**
GDA Issue Action	Implement the proposed modification to provide a diverse low RCP speed trip signal on an appropriately diverse protection system for a reduction in flow fault with failure of the reactor protection system to trip. EDF and AREVA have identified that a modification is required to provide a reactor trip signal on low RCP speed on a non-TXS based protection system. This is to protect against a flow reduction fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A4**
GDA Issue Action	Implement the proposed modification to provide diverse high axial offset and high neutron flux trips on an appropriately diverse protection system for a RCCA bank withdrawal fault with failure of the reactor protection system to trip. EDF and AREVA have identified that two extra reactor trip signals need to be added to a non-TXS based protection system. The extra trip signals are a high axial offset trip and a high neutron flux trip. These changes are to protect against a RCCA bank withdrawal fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
GI-UKEPR-FS-02 – REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A5**
GDA Issue Action	Demonstrate the provision of diverse protection against rod misplacement faults including one or more dropped rods. No analysis of these faults is presented within NEPR-F DC 592 and yet these faults will be very difficult to detect should there be a failure of the TXS-based reactor protection system. For this reason, EDF and AREVA are to provide explicit transient analysis using design basis analysis techniques for these faults to demonstrate that the diverse protection systems are functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a negative-rate flux trip signal on a non TXS-based protection system is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A6**
GDA Issue Action	Demonstrate the provision of diverse protection against loss of CVCS following a normal reactor trip and xenon decay including demonstration of diversity to operator action. After every reactor trip from full power there is an eventual decay in the level of xenon poisoning within the reactor core. The resultant swing in reactivity needs to be compensated for through increasing the boron concentration in the reactor to ensure an adequate shutdown margin. While the emergency boration system (EBS) and the in-containment refuelling water storage tank (IRWST) provide two diverse sources of borated water, should the operator fail to ensure adequate shutdown margin using the Chemical and Volume Control System (CVCS), both these systems are also dependent upon operator action for actuation. Although timescales are long (many hours), this implies a combined human reliability of 1×10^{-7} per demand to meet the design basis target. For this reason, EDF and AREVA are to provide an ALARP study into the feasibility of automatically actuating the CVCS system to inject borated water after every reactor trip and for the EBS to be automatically actuated following failure of the CVCS. Alternatively, EDF and AREVA may wish to provide a consequence analysis of what would happen should the operator fail to ensure adequate shutdown margin. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A7**
GDA Issue Action	Demonstrate the provision of diverse protection against a homogenous boron dilution fault occurring in shutdown conditions with failure of the reactor protection system. No analysis of this fault is presented within NEPR-F DC 592 and yet such a fault would be very difficult to detect should there be a failure of the TXS-based reactor protection system. For this reason, EDF and AREVA are to provide explicit transient analysis using design basis analysis techniques for this fault to demonstrate that the diverse protection systems are functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a boron dilution block signal and an EBS actuation signal on a non TXS-based protection system (actuated by low doubling time and/or high source-range flux level) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A8**
GDA Issue Action	Demonstrate the provision of diverse protection for the frequent faults involving the loss of essential support systems (e.g. loss of cooling chain, electrical, HVAC). EDF and AREVA are to provide a demonstration of diversity for frequent faults involving loss of essential support systems including loss of cooling chain, electrical and HVAC systems. EDF and AREVA are to demonstrate that any diverse systems claimed are appropriately categorised. In the case of loss of grid with failure of the TXS-based protection system, the feasibility of automatically actuating the station-blackout diesel generators (SBO DGs) on a non-TXS based protection system will need to be considered as a possible ALARP measure. Any design changes identified from the review will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

GI-UKEPR-FS-02 – REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A9**
GDA Issue Action	Demonstrate that there exists a diverse means of achieving the safe shutdown state from the controlled state for frequent faults. EDF and AREVA are to demonstrate that diverse means of achieving a safe shutdown state from the controlled state exist for all frequent faults and that all structures, systems and components are appropriately categorised. Any design changes required because of any reclassifications will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

SPENT FUEL POOL SAFETY CASE

GI-UKEPR-FS-03 Revision 2

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Mechanical Engineering Structural Integrity Internal Hazards		
GDA Issue Reference	**GI-UKEPR-FS-03**	**GDA Issue Action Reference**	**GI-UKEPR-FS-03.A1**
GDA Issue	The safety case for the spent fuel pool is to be extended to consider faults associated with the Cask Loading Pit and leaks currently excluded from the design basis by break preclusion arguments.		
GDA Issue Action	EDF and AREVA to evaluate Cask Loading Pit Initiating Events. They need to determine the updates required to DBA or PSA safety cases for faults associated with the cask loading pit. A FMECA (Failure Modes, Effects and Criticality Assessment) should be performed to determine failure modes leading to the fault events. For each fault, initiating events and sequences leading to a faulty state need to be determined. Frequencies associated to each initiating event need to be determined. Faults needed to be added to the PSA and/or DBA safety cases appropriately. A report should be provided to ONR presenting the considered initiating events, sequences and attributed frequencies. This report should identify for each family of faults if it will be included in the PSA and DBA safety cases. The relative importance of administrative controls, interlocks, equipments, equipment classification, operator actions and associated claims should be included and described. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

SPENT FUEL POOL SAFETY CASE

GI-UKEPR-FS-03 Revision 2

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Mechanical Engineering Structural Integrity Internal Hazards		
GDA Issue Reference	**GI-UKEPR-FS-03**	**GDA Issue Action Reference**	**GI-UKEPR-FS-03.A2**
GDA Issue Action	EDF and AREVA to provide an updated safety case for the spent fuel pool, incorporating the faults associated with the cask loading pit. The safety case needs to formalised: • If new PSA initiating events are identified by Action 1, additional event trees need to be incorporated into the PSA model. • If additions to the DBA are required: the category of the additional events (PCC-3/4) should be determined and adequate calculations or ALARP analysis undertaken to ensure that all criteria are met. A report should be provided to ONR describing the proposed changes to the safety case. EDF and AREVA shall update the PCSR accordingly with the agreed safety case developed through Action 1 and this Action. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

SPENT FUEL POOL SAFETY CASE

GI-UKEPR-FS-03 Revision 2

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Mechanical Engineering Structural Integrity Internal Hazards		
GDA Issue Reference	**GI-UKEPR-FS-03**	**GDA Issue Action Reference**	**GI-UKEPR-FS-03.A3**
GDA Issue Action	EDF and AREVA shall provide a consequences analysis for spent fuel pool leaks previously not considered within the design basis because of break preclusion arguments. EDF and AREVA identify a number of leaks associated with spent fuel pool which are currently excluded from the design basis analysis presented in the PCSR by evoking a break preclusion concept. The rigour required to show that the likelihood of failure is so low that the consequences of failure can be discounted is high in UK and should not be put forward to avoid making a consequences analysis. While a small number of High Integrity Components (HIC) have been recognised associated with the primary reactor circuit, the safety case as currently presented does not identify the spent fuel pool components as part of the HIC envelope. A consequences analysis of the identified leaks is to be provided, and a safety case (with accompanying ALARP arguments) identifying the design features and systems required to ensure the consequences are acceptable shall be submitted to ONR for assessment. The PCSR is to be updated to reflect any changes in the safety case. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Structural Integrity Human Factors Control and Instrumentation		
GDA Issue Reference	**GI-UKEPR-FS-04**	**GDA Issue Action Reference**	**GI-UKEPR-FS-04.A1**
GDA Issue	The safety case for steam generator tube rupture faults needs revising to incorporate significant design changes identified by EDF and AREVA. The safety case should demonstrate that the proposed detection and management strategy is ALARP and provide justification for the claims on operation actions. If the analysis shows that the proposed strategy is not ALARP, then alternative strategies will need to be developed.		
GDA Issue Action	EDF and AREVA to provide a revised safety case and an ALARP argument to ONR to justify their proposed design to detect and mitigate PCC-3 Steam Generator Tube Ruptures. EDF and AREVA need to provide additional arguments and evidence to justify their design approach for PCC-3 SGTR faults or propose an alternative strategy. Therefore: • more information on the safety classification of these manual actions is required and an ALARP argument as to why they cannot be automated is to be provided; or • if an alternative strategy is identified, this similarly needs to be fully justified and substantiated, including new transient analysis. Any proposed modification arising from the above is to be handled through the agreed process for managing design change in GDA. EDF and AREVA shall update the PCSR and Fault Schedule in accordance with the agreed safety case. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Structural Integrity Human Factors Control and Instrumentation		
GDA Issue Reference	**GI-UKEPR-FS-04**	**GDA Issue Action Reference**	**GI-UKEPR-FS-04.A2**
GDA Issue Action	EDF and AREVA to provide a detailed human factors justification of the actions claimed in the design basis safety case for the PCC-3 fault. In support of the ALARP case required in Action 1, a detailed human factors justification of any manual actions claimed in the design basis safety case for the PCC-3 fault is to be submitted to ONR-ND. SGTR faults are amongst the most challenging events to ONR's Target 4 for design basis fault sequences because of the potential for radioactive products to be discharged to atmosphere through the main steam relief train. EDF and AREVA have proposed a new mitigation strategy for the PCC-3 fault that departs from the typical UK EPR safety case principle of relying on automatic F1A (Class 1) actions to reach the controlled state. In addition to a manual reactor trip, the current proposals require the operator to perform additional manual actions such as isolation of the affected SG, start of the EFW. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Structural Integrity Human Factors Control and Instrumentation	
GDA Issue Reference	**GI-UKEPR-FS-04**	**GDA Issue Action Reference**	**GI-UKEPR-FS-04.A3**
GDA Issue Action	EDF and AREVA to provide transient analysis to show that there is a margin to overfill for the design basis PCC-3 and PCC-4 SGTR faults, with assumptions appropriate for the UK EPR. The UK EPR design has diverged away from the analysis presented in the PCSR to such an extent that new analyses of the PCC-3 2A-SGTR and PCC-4 4A-SGTR events are required to demonstrate there is a margin to overfill and that the long term safe shutdown state can be reached with safety criteria met. EDF and AREVA shall update the PCSR to reflect the revised analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN BASIS ANALYSIS OF ESSENTIAL SUPPORT SYSTEMS

GI-UKEPR-FS-05 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Electrical Engineering		
GDA Issue Reference	**GI-UKEPR-FS-05**	**GDA Issue Action Reference**	**GI-UKEPR-FS-05.A1**
GDA Issue	EDF and AREVA to provide a design basis analysis of failures in the essential support systems.		
GDA Issue Action	EDF and AREVA to perform a design basis analysis of the following initiating events on the essential support systems of the UKEPR: • Loss of cooling chain faults as identified in NEPR-F DC 584 Rev A. • Electrical system faults (as identified from future PSA screening analysis). • HVAC system faults (as identified from future PSA screening analysis). EDF and AREVA have identified a number of cooling chain failures that need to be treated as design basis initiating events within the PCC analysis. These faults should be subject to a design basis analysis. EDF and AREVA have identified that failures in the electrical system and HVAC system have still to be analysed within the PSA. However, at this stage, a simplified screening analysis will be performed for initiating events related to Electrical system faults and HVAC system faults. Once the simplified PSA screening analysis is complete, any new initiating bounding events identified must be reviewed for consideration as design basis events. Any new design basis initiating events that are identified shall be subject to a design basis analysis (PGI-UKEPR-FS.2.A8). In particular, for any design basis event associated with failures in these essential support systems, EDF and AREVA must demonstrate the functional capability of the associated protection systems and that these have an appropriate safety categorisation. Any shortfall in requirements shall be subject to an ALARP analysis to identify possible design improvements to reach the appropriate standard. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

Further explanatory / background information on the GDA Issues for this topic area can be found at:	
GI-UKEPR-FS-01 Revision 0	Ref. 93.
GI-UKEPR-FS-02 Revision 0	Ref. 94.
GI-UKEPR-FS-03 Revision 2	Ref. 95.
GI-UKEPR-FS-04 Revision 1	Ref. 96.
GI-UKEPR-FS-05 Revision 0	Ref. 97.