Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

GDA Close-out for the EDF and AREVA UK EPR™ Reactor

GDA Issue GI-UKEPR-FS-05 Revision 0 – Design Basis Analysis of Essential Support Systems

Assessment Report: ONR-GDA-AR-12-013
Revision 0
March 2013

COPYRIGHT

First published March 2013

EXECUTIVE SUMMARY

This report presents the close-out of part of the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) within the area of Fault Studies design basis analyses. This report specifically addresses the GDA Issue **GI-UKEPR-FS-05** Revision 0 generated as a result of the GDA Step 4 Fault Studies Assessment of the UK EPR™. The assessment has focused on the deliverables identified within the EDF and AREVA Resolution Plan published in response to the GDA Issue.

During the GDA assessment it became apparent that EDF and AREVA had not provided a design basis safety case for loss of essential support system faults within the Pre-Construction Safety Report (PCSR). For this reason, **GI-UKEPR-FS-05** was raised requiring EDF and AREVA to provide such a case.

In response to GDA Issue **GI-UKEPR-FS-05**, EDF and AREVA have produced a design basis safety case for loss of essential support system faults on the UK EPR™. The development of this safety case has necessitated EDF and AREVA reviewing all the essential support systems on the UK EPR™ including the essential electrical systems, the Heating, Ventilation and Air Conditioning (HVAC) systems, the instrument air systems, the nitrogen gas distribution systems, and the cooling chain systems comprising the Component Cooling Water System (CCWS) and the Essential Service Water System (ESWS). For each system, EDF and AREVA have considered the implications of both their partial or complete failure. This work has resulted in the identification of a significant number of design changes to the essential support systems.

My assessment has focused on:

- The functional analysis performed in support of the design basis analysis for loss of essential support system faults on the UK EPR™. In particular, I have focused on whether adequate functional diversity is provided within the design of the essential support systems so as to minimise the likelihood of common mode failure of these important systems.
- The transient analysis studies used to demonstrate that sufficient front line systems remain available to reach the safe shutdown state following either the partial or complete loss of each essential support system.

In some areas there has been a lack of detailed information which has limited the extent of my assessment. As a result, the Office for Nuclear Regulation (ONR) will need additional information to underpin my judgements and conclusions and these are identified in 31 Assessment Findings to be carried forward as normal regulatory business. These are listed in 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 the close-out phase of GDA and made significant progress against GDA Issue **GI-UKEPR-FS-05** covering the loss of essential support system faults identified in my GDA Step 4 assessment report.

In my opinion, EDF and AREVA have considerably strengthened the design basis safety case against loss of essential support system faults for the UK EPR™ through the additional safety case analysis performed in response to GDA Issue **GI-UKEPR-FS-05**. This has included systematically reviewing the consequences of single failures and common mode failures on each of the essential support systems. The work has been supported by the performance of additional transient analysis studies to demonstrate that sufficient front line systems remain available to reach the safe shutdown state following such failures.

The analytical work performed by EDF and AREVA has been aided by a number of important design changes to the essential support 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 changes identified are (in order of assessment in this report):

- Upgrade of the automatic switchover from the operating CCWS / ESWS train to the stand-by CCWS / ESWS train on loss of the operating train to Class 1.
- Upgrade of the automatic isolation of the operating CCWS / ESWS train from the common auxiliaries header in case of leakage to Class 1.
- Upgrade of the automatic trip on the Reactor Coolant Pumps (RCP) on low injection flow rate to the seals or high thermal barrier temperature to Class 1.
- Upgrade of the automatic switchover of the cooling of the Low Head Safety Injection (LHSI) pumps 1 and 4 from the CCWS to the safeguard building chilled water system on low CCWS flow rate or high CCWS temperature to Class 1.
- Upgrade of the manual realignment of the Emergency Feedwater System (EFWS) common pump discharge headers from a local to plant action to a main control room action at Class 1.
- Addition of a common header on the CCWS lines cooling the Reactor Coolant Pump (RCP) thermal barriers.
- Upgrade of the safeguard building chilled water system to Class 1.
- Upgrade of the safeguard building ventilation system to Class 1.
- Creation of a new Class 2 safeguard building diverse chilled water system allocated to divisions 1 and 4 of the 400V AC essential electrical system that will be housed in an extra single storey to be added to safeguard buildings 1 and 4.
- Creation of a new Class 1 safeguard building diverse ventilation system allocated to divisions 1 and 4 of the 400V AC essential electrical system.
- Upgrade of the automatic switchover from the safeguard building ventilation system to the safeguard building new diverse ventilation system on loss of normal systems to Class 1.
- Upgrade of the automatic switchover from the safeguard building chilled water system to the safeguard building new diverse chilled water system on loss of normal systems to Class 2.
- Upgrade of the main control room air conditioning system to Class 1.
- Upgrade of the high temperature alarms in the ESWS shaft of the pumping station to Class 1.
- Implementation of a back-up electrical supply to the Extra Boration System (EBS) trains and associated C&I and support systems.
- A reallocation of the electrical supplies of the CCWS common isolation valves on trains 1 and 4 to the 220V DC essential electrical system.
- A reallocation of the electrical supplies of the ESWS heat exchanger regulation valves on trains 1 and 4 to the 220V DC essential electrical system.
- A reallocation of the electrical supplies for one of the common isolation valves on each train of the steam generator blowdown system to the 220V DC essential electrical system.

- A reallocation of the electrical supplies of one of the two pumps on each train of the Fuel Pool Cooling System (FPCS) to the 400V AC essential electrical system.
- A reallocation of the electrical supplies of the safeguard building diverse chilled water system to the 400V AC essential electrical system.

In my judgement any additional design changes that may result from the closure of Assessment Findings are likely to be limited to changes in the allocation of electrical loads in two out of the four electrical divisions in the safeguard buildings and changes in the C&I control systems for the HVAC systems. Given the potential implications to plant layout of these changes, it is considered essential that this analysis and design work is substantially completed early in the site specific detailed design phase and prior to the issue of Consent to start the pouring of Nuclear Island safety-related concrete.

Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that sufficient progress has been made on the safety case for loss of essential support system faults presented in the supporting documentation submitted in response to GDA Issue **GI-UKEPR-FS-05** to justify its closure subject to satisfactory progression and resolution of the Assessment Findings identified in Annex 2. These are to be addressed during the forward work programme for this reactor. For this reason, I am satisfied that GDA issue **GI-UKEPR-FS-05** can now be closed.

LIST OF ABBREVIATIONS

AC	Alternating Current
ALARP	As Low As Is Reasonably Practicable
C&I	Control and Instrumentation
CCWS	Component Cooling Water System
CHRS	Containment Heat Removal System
CMF	Change Management Form
CVCS	Chemical and Volume Control System
CW	Circulation Water
CWFS	Circulation Water Filtration System
DC	Direct Current
DNB	Departure from Nucleate Boiling
EBS	Extra Boration System
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System
ESWS	Essential Service Water System
FA3	Flamanville 3 (Nuclear Power Plant)
FPCS	Fuel Pool Cooling System
GDA	Generic Design Assessment
HSE	Health and Safety Executive
HVAC	Heating Ventilation and Air Conditioning (System)
IRWST	In-containment Refuelling Water Storage Tank
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
MCR	Main Control Room
MHSI	Medium Head Safety Injection
MSRT	Main Steam Relief Train
NCSS	Non-Computer based Safety System
ONR	Office for Nuclear Regulation (an agency of HSE)
PCC	Plant Condition Category
PCSR	Pre-Construction Safety Report
PORV	Power Operated Relief Valve

LIST OF ABBREVIATIONS

PS	Protection System
PSA	Probabilistic Safety Analysis
PSV	Pressuriser Safety Valve
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RRC-A	Risk Reduction Category A
RRC-B	Risk Reduction Category B
RBWMS	Reactor Borated Water Make-up System
SABL	Safety Analysis Bounding Limit
SAP	Safety Assessment Principle(s) (HSE)
SAS	Safety Automation System
SBLOCA	Small Break Loss of Coolant Accident
SBO	Station Blackout
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIS	Safety Injection System
SSSS	Stand-Still Seal System
TAG	Technical Assessment Guide(s) (ONR)
TLOCC	Total Loss of Cooling Chain
TQ	Technical Query
TSC	Technical Support Contractor
TXS	C&I Digital Computer Platform
UCWS	Ultimate Cooling Water System
UDG	Ultimate Diesel Generator
UPS	Uninterruptible Power Supply

TABLE OF CONTENTS

Annexes

1 INTRODUCTION

1.1 Background

1 This report presents the close-out of part of the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) within the area of Fault Studies design basis analyses. This report specifically addresses the GDA Issue **GI-UKEPR-FS-02** Revision 0 and associated Actions (Ref. 1) generated as a result of the GDA Step 4 Fault Studies Assessment of the UK EPR™ (Ref. 2). The assessment has focused on the deliverables identified within the EDF and AREVA Resolution Plan (Ref. 3) published in response to the GDA Issue.

2 GDA followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by EDF and AREVA were examined and in Step 3 the arguments that underpin those claims were examined. The Step 4 assessment reviewed the safety aspects of the UK EPR™ reactor in greater detail, by examining the evidence, supporting the claims and arguments made in the safety documentation.

3 The Step 4 Fault Studies Assessment identified five GDA Issues and a number of Assessment Findings as part of the assessment of the evidence associated with the UK EPR™ reactor design. A GDA Issue is an observation of particular significance that requires resolution before the Office for Nuclear Regulation (ONR), an agency of HSE, would agree to the commencement of nuclear safety related construction of the UK EPR™ within the UK. An Assessment Finding results from a lack of detailed information which has limited the extent of assessment and as a result the information is required to underpin the assessment. However, they are to be carried forward as part of normal regulatory business.

4 During the GDA assessment it became apparent that EDF and AREVA had not provided a design basis safety case for loss of essential support system faults within the PCSR. For this reason, **GI-UKEPR-FS-05** was raised requiring EDF and AREVA to provide such cases.

5 The aim of this assessment is to provide a comprehensive assessment of the submissions provided in response to GDA Issue **GI-UKEPR-FS-05** to enable ONR to gain confidence that the concerns raised have been resolved sufficiently so that the issue can either be closed or lesser safety significant aspects be carried forward as Assessment Findings.

1.2 Scope of Assessment

6 The scope of this assessment differs from that adopted for the previous reports produced within GDA, most notably the Step 4 Fault Studies Assessment. This report presents the assessment of an individual GDA Issue rather than a report detailing close-out of all five GDA Issues associated with the technical area of Fault Studies. The reasoning behind adopting this approach is to allow closure of GDA Issues as the work is completed rather than having to wait for the completion of all the GDA work in this technical area.

7 Further to the assessment work undertaken during Step 4 (Ref. 2), and the resulting GDA issue **GI-UKEPR-FS-05** (Ref. 1), this assessment focuses on:

- The functional analysis performed in support of the design basis analysis for loss of essential support system faults on the UK EPR™. In particular, I have focused on whether adequate functional diversity is provided within the design of the essential support systems so as to minimise the likelihood of common mode failure of these important systems.

- The transient analysis studies used to demonstrate that sufficient front line systems remain available to reach the safe shutdown state following either the partial or complete loss of each essential support system.

8 The purpose of this assessment is to consider whether the deliverables provided in response to the GDA Issue, **GI-UKEPR-FS-05**, and the associated GDA Issue Action, provide an adequate response sufficient to justify closure of the issue. The GDA Issue and its action are detailed within Annex 3 of this report. As such, this report presents only the assessment undertaken as part of the resolution of this GDA Issue and it is recommended that this report be read in conjunction with the Step 4 Fault Studies Assessment of the EDF and AREVA UK EPR™ in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process (Ref. 2).

9 Specifically, this assessment report is not intended to revisit aspects of assessment already undertaken and confirmed as being adequate during previous stages of the GDA. However, should evidence from the assessment of EDF and AREVA's responses to GDA Issues highlight shortfalls not previously identified during Step 4, there will be a need for these aspects of the assessment to be highlighted and addressed as part of the close-out phase or be identified as Assessment Findings to be taken forward to site specific detailed design phase.

10 The possibility of further Assessment Findings being generated as a result of this assessment is not precluded given that resolution of the GDA Issues may identify areas where further detailed evidence will be required when the information becomes available at a later stage of the design process.

1.3 Assessment Methodology

11 The methodology applied to this assessment is identical to the approach taken during Step 4 and follows ONR guidance and procedures (Ref. 4).

12 This assessment has been focused primarily on the submissions relating to resolution of the GDA Issues as well as any further requests for information or justification derived from assessment of those specific deliverables.

1.4 Structure of Report

13 The structure of the report is as follows. In Section 2, the strategy adopted for this Fault Studies assessment is set out. In Section 3, the deliverables provided by EDF and AREVA in response to the GDA Issue as detailed within their resolution Plan (Ref. 3) are briefly summarised. My assessment of EDF and AREVA design basis safety case for loss of essential support system faults is presented in Section 4. The conclusions of this Fault Studies assessment are presented in Section 5. Section 6 lists the Assessment Findings.

2 ONR'S ASSESSMENT STRATEGY FOR THE LOSS OF ESSENTIAL SUPPORT SYSTEM FAULTS SAFETY CASE

2.1 Assessment Plan

14 The intended assessment strategy for GDA Close-out of the Fault Studies topic area was set out in an assessment plan (Ref. 5). The assessment plan, which is based upon the GDA issues from the GDA Step 4 Assessment Report (Ref. 2), identifies the intended scope of the assessment and the standards and criteria that would be applied. The assessment strategy is summarised in the following sub-sections.

2.2 Standards and Criteria

15 Judgements have been made against the 2006 HSE Safety Assessment Principles (SAP) for Nuclear Facilities (Ref. 6). In particular, the fault analysis and design basis accident SAPs (FA.1 to FA.9), the severe accident 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) have been considered. In addition, the following Technical Assessment Guides (TAG) have been used as part of this assessment (Ref. 7):

- T/AST/034 – Transient analysis for Design Basis Accidents in Nuclear Reactors
- T/AST/042 – Validation of Computer Codes and Calculational Methods

16 EDF and AREVA have assessed the safety case against their own design requirements.

2.3 The Approach to Assessment for GDA Close-out

17 The overall basis for the assessment of the GDA Issue **GI-UKEPR-FS-05** are the Fault Studies elements of the following documents:

- Submissions made to ONR in accordance with the resolution plans.
- The specific updates made to the Submission / Pre-construction Safety Report (PCSR) / Supporting Documentation associated with the loss of essential support system faults safety case.
- The Design Reference that relates to the Submission / PCSR as set out in UK EPR™ GDA Project Instruction UKEPR-I-002 (Ref. 8) which has been updated throughout GDA Issue resolution to include Change Management Forms (CMF).
- In addition to, and as result of, the assessment of the submissions made in accordance with the resolution plan, a Technical Query (TQ) was issued. The response made by EDF and AREVA to the TQ (Ref. 9) has been subjected to detailed assessment against the same standards and criteria.

18 The objective of the fault studies assessment has been to assess submissions made by EDF and AREVA in response to the GDA Issue identified through the GDA process and the design changes proposed by EDF and AREVA and, if judged acceptable, clear the GDA Issue.

2.3.1 Use of Technical Support Contractors

19 No Technical Support Contractors (TSC) were utilised in the assessment of this GDA Issue.

2.3.2 Cross-cutting Topics

20 Fault analysis, by its very nature, tends to interface with many of the technical areas associated with a safety case. During Step 4, a number of areas have been identified as "cross-cutting topics". This practice has continued during the close-out of this issue and so the assessment work has been co-ordinated with the Probabilistic Safety Analysis (PSA) (Ref. 10) and the Control and Instrumentation (C&I) and Electrical Engineering (Refs 11 & 12) topic leads.

2.3.3 Out of Scope Items

21 During Step 4 (Ref. 2), a number of items were identified as being outside the scope of GDA. One of these, the development of suitable Operational Technical Specifications, is relevant to the loss of essential support system faults design basis safety case.

3 EDF AND AREVA DELIVERABLES IN RESPONSE TO THE GDA ISSUE

22 The information provided by EDF and AREVA in response to this GDA Issue, as detailed within their Resolution Plan (Ref. 3), was broken down under Action 1 of the GDA Issue into the following specific deliverables for detailed assessment

GDA Issue Action	Technical Area	Deliverable	Ref.
GI-UKEPR-FS-05.A1	Functional Analysis of single failures (i.e. partial loss) of essential support systems	Report A – Design Basis Analysis of single fault on essential support systems	13
GI-UKEPR-FS-05.A1	Probabilistic Analysis of Safeguard Building HVAC systems	Report B – Probabilistic assessment of the initiating events relative to the loss of DVL and DEL trains in the frame of the GDA issue GI-UKEPR-FS-05	14
GI-UKEPR-FS-05.A1	Transient Analysis of single failures (i.e. partial loss) of essential support systems	Report C – Loss of support systems – Transient Analysis	15
GI-UKEPR-FS-05.A1	As low as is reasonably practicable (ALARP) Review	Report D – GDA FS-05 – Faults in Essential Support Systems – ALARP Assessments, Proposed Design Changes and Justification of Resultant Design	16
GI-UKEPR-FS-05.A1	Functional analysis of complete loss of cooling chain (Total Loss of Cooling Chain – TLOCC)	Report E – EPR™ UK GDA – GDA issue FS-05 – Safety frame for common cause failure events on the cooling chain, and analysis of classification upgrade of TLOCC mitigation means	17
GI-UKEPR-FS-05.A1	Probabilistic analysis of complete and partial loss of essential electrical systems initiating event frequencies	Report F – Identification of single and common modes of failure for the electrical systems for the UK EPR GDA issue FS-05	18
GI-UKEPR-FS-05.A1	Conceptual Design for Safeguard Building HVAC systems	Report G –GDA – DVL / DEL – Conceptual design note.	19
GI-UKEPR-FS-05.A1	Functional Analysis of loss of other HVAC systems	Report I – Screening of the HVAC systems to establish the impact of their loss on normal operation systems and on safety systems.	20
GI-UKEPR-FS-05.A1	Functional Diversity for Frequent Faults	Report J – Response to GI-UKEPR-FS-02 – Actions 8 and 9 – Diversity for frequent faults and to GI-UKEPR-FS-05 Action 1 – Loss of support systems.	21
GI-UKEPR-FS-05.A1	PCSR – Sub-Chapter 3.2 PCSR – Sub-Chapter 6.6 PCSR – Sub-Chapter 9.2 PCSR – Sub-Chapter 9.4 PCSR – Sub-Chapter 14.7 PCSR – Sub-Chapter 16.4 PCSR – Sub-Chapter 18.2	Classification of Structure, Equipment and Systems Emergency Feedwater System Water Systems HVAC Systems Fault and Protection Schedule Specific Studies Normal Operation	22

23 A brief overview of each of the deliverables is provided within this section. It is important to note that this information is supplementary to the information provided within the November 2009 PCSR (Ref. 23) which has already been subject to detailed assessment during earlier stages of GDA. The deliverables are intended to provide a preliminary safety case for loss of essential support system faults on the UK EPR™ suitable for GDA.

Design Basis Analysis of Single Fault on Essential Support Systems

24 This report (Ref. 13) presents the functional analysis of single failure (i.e. partial loss) of the systems comprising the cooling chain, the safeguard building main Heating, Ventilation, and Air Conditioning (HVAC) system, the safeguard building essential electrical system, the instrument air system, and the nitrogen gas distribution system. A deterministic assessment is performed in which the most onerous single failure and plant maintenance condition are assumed together with consequential Loss of Off-site Power (LOOP) following a reactor trip caused by the partial loss of an essential support system.

Probabilistic Assessment of the Initiating Events relative to the loss of DVL and DEL trains

25 This report (Ref. 14) presents a probabilistic assessment to determine the initiating event frequencies for both the partial and complete loss of the safeguard building main HVAC systems. The results of a fault and event tree analysis of the safeguard building main HVAC system are presented.

Loss of Support Systems – Design Basis Analyses

26 This report (Ref. 15) presents the transient analysis studies performed in support of the deterministic assessment of single faults on the essential support systems. Two design basis faults are analysed. These are the trip of two Reactor Coolant Pumps (RCPs) together with the loss of three safeguard divisions and a seal Loss of Coolant Accident (LOCA) fault on all four RCPs together with the loss of three safeguard divisions.

ALARP Assessments, Proposed Design Changes and Justification of Resultant Design

27 The purpose of this report (Ref. 16) is to summarise the findings of all the other reports produced in response to **GI-UKEPR-FS-05** and where shortfalls are identified to perform an ALARP assessment to identify the potential design changes to improve the protection provided. The report acknowledges that many of the proposals are still under review and that further work will be required during the site specific detailed design phase.

Safety Frame for Common Cause Failure on the Cooling Chain, and Analysis of Classification Upgrade of TLOCC Mitigation Means

28 This report (Ref. 17) considers the specific case of total loss of cooling chain due to common mode failure of either the Component Cooling Water System (CCWS) or the Essential Service Water System (ESWS). It identifies a number of design changes required to meet deterministic criteria.

Probabilistic Analysis of Complete and Partial Loss of Essential Electrical Systems Initiating Event Frequencies

29 This report (Ref. 18) presents a probabilistic assessment to determine the initiating event frequencies for both the partial and complete loss of the essential electrical systems.

DVL / DEL Conceptual Design Note

30 The purpose of this report (Ref. 19) is to present a conceptual design for the proposed re-design of the safeguard building main and diverse HVAC systems. The note identifies high level safety functional requirements for the proposed HVAC systems together with the requirements for the associated C&I, electrical, and mechanical equipment.

Screening of the HVAC Systems to establish the impact of their loss on normal operation systems and on safety systems

31 This report (Ref. 20) presents a screening analysis of the remaining HVAC systems other than the safeguard building main HVAC systems. A high level analysis is performed to review the consequences of common mode failure events. The potential for such an event to initiate a reactor transient and whether the transient is bounded by an existing Plant Condition Category (PCC) design basis event are identified.

Diversity for Frequent Faults – Loss of Support Systems

32 The purpose of this letter (Ref. 21) is to demonstrate that diverse protection exists on the UK EPR™ following frequent loss of essential support system faults such as the loss of one train of the CCWS, loss of one division of the safeguard building HVAC system, or one division of the safeguard building essential electrical system. The letter has been produced in response to Action 8 of GDA issue **GI-UKEPR-FS-02** as well as GDA Issue **GI-UKEPR-FS-05**.

PCSR Updates

33 In addition to the technical reports, EDF and AREVA have also provided updates (Ref. 22) to the March 2011 PCSR (Ref. 24). These consist of Sub-Chapter 3.2 on the classification of structures, equipment and systems, Sub-Chapters 6.6, 9.2 and 9.4 incorporating changes to the Emergency Feedwater System (EFWS), the water systems (CCWS, ESWS) and HVAC systems respectively, Sub-Chapter 14.7 on the fault and protection schedule, Sub-Chapter 16.4 with a specific section of loss of essential support system faults and Sub-Chapter 18.2 on normal operation (including the maintenance programme).

4 ONR ASSESSMENT

34 My assessment against the SAPs of the UK EPR™ loss of essential support system faults safety case is presented below.

35 The assessment commences in Section 4.1 with an assessment of the safety case for the partial and complete loss of the main cooling chain systems. Assessment of the safety case for the partial and complete loss of the safeguard building main HVAC system is presented in Section 4.2 while Section 4.3 assesses the safety case for all other HVAC systems. Sections 4.4 and 4.5 assess the safety cases for the complete loss of the instrument air system and the nitrogen gas distribution system respectively. The safety case for the partial and complete loss of essential electrical systems is considered in Section 4.6. Section 4.7 provides a brief review of the updates to those areas of the PCSR concerning the loss of essential support system faults.

36 In some areas there has been a lack of detailed information which has limited the extent of my assessment. As a result, ONR 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 2.

4.1 Loss of Cooling Chain Systems Safety Case

4.1.1 Summary of EDF and AREVA's Safety Case

37 Faults in this category result in the total or partial loss of the CCWS and ESWS systems. Such faults can potentially produce multiple consequences. For example, the loss of the CCWS may result in the loss of cooling to the RCP seals causing a Small Break Loss of Coolant Accident (SBLOCA) in case of failure of the Stand-Still Seal System (SSSS) and failure of cooling to the In-containment Refuelling Water Storage Tank (IRWST) if the Containment Heat Removal System (CHRS) is not activated with consequential loss of the safety injection systems such as the Medium Head Safety Injection (MHSI) system and the Low Head Safety Injection (LHSI) system with the potential for the core to become uncovered.

38 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 either partial or complete loss of either the CCWS or the ESWS systems that make-up the cooling chain. For those cases which they consider to be limiting, they have performed detailed analyses.

39 In the case of partial loss of either the CCWS or the ESWS, EDF and AREVA claim that these studies demonstrate that adequate redundancy is provided on the UK EPR™ even after taking account of the most onerous single failure, the worst plant maintenance state and the assumed consequential loss of off-site power, such that at least one of the safeguard divisions remains available and that this is sufficient to provide adequate cooling of the reactor even assuming seal LOCAs in all four RCPs.

40 In the case of complete loss of either the CCWS or the ESWS, EDF and AREVA claim that each of the chilled water trains in Divisions 1 or 4 of the safeguard building main HVAC system can be air-cooled and can provide adequate cooling to the LHSI pumps while the diverse CHRS and Ultimate Cooling Water System (UCWS) located in Divisions 1 and 4 provide cooling to the IRWST. The decay heat removal function is performed by the EFWS pumps which are also located in Divisions 1 and 4 and which are self-cooling. EDF and AREVA claimed that the decay heat removal function and boration

function can be performed even assuming seal LOCAs in all four RCPs and the worst plant maintenance state.

41 On the basis of the analysis presented, EDF and AREVA have concluded that adequate protection against loss of cooling chains faults is provided for all the range of faults considered.

4.1.2 Assessment

42 EDF and AREVA have identified the following faults within this category that they consider to be the limiting single failures (Refs 13 and 16):

- Mechanical failure of a single CCWS / ESWS train.
- Break in a single CCWS / ESWS train.
- Break in a single CCWS common header.

43 In addition, EDF and AREVA identify the following faults within this category that they consider to be the limiting common mode failures (Refs 16 and 17):

- Total loss of all four CCWS trains.
- Total loss of all four ESWS trains.

44 In the sections below, I have separately presented my assessment of partial failure of a cooling chain system (Section 4.1.2.1) from my assessment of total failure of a cooling chain system (Section 4.1.2.2).

4.1.2.1 Partial Loss of a Cooling Chain System

System Description of the Cooling Chain Systems

45 Before reviewing the fault sequence analysis for this fault it is worth reviewing the system designs for the CCWS and the ESWS.

46 The role of the CCWS is to cool the following components:

Group 1

- The bearings and motors of the LHSI, MHSI, CCWS pumps
- The LHSI heat exchangers.

Group 2

- The fuel pool cooling system (FPCS) heat exchangers.
- The heat exchangers of the chilled water trains on the safeguard building main HVAC system in Divisions 2 and 3.
- The thermal barrier of the RCPs.

47 The CCWS also cools the following components which EDF and AREVA judge have less safety significance:

Group 3

- The bearing and motors of the RCPs.

- The bearings and motors of the chemical volume control system (CVCS) and the reactor borated water make-up system (RBWMS) pumps.
- The heat exchangers of the CVCS, RBWMS, the sampling system, and the operational chilled water system.

Group 4

- Other non-safety classified systems.

48 The CCWS is a four train system that is supplied from four independent electrical trains. Each train of the CCWS is associated with one train of Group 1 components and is cooled by one train of the ESWS. However, it also shares two common headers (and associated loads) with a second CCWS train (i.e. CCWS trains 1 and 2 share common loads 1a and 1b and CCWS trains 3 and 4 share common loads 2a and 2b). Each CCWS train can be isolated from these common loads. These common loads cool the components in Groups 2, 3 and 4. During normal operation only the pumps on two of the CCWS / ESWS trains are in operation with the others on standby (i.e. either train 1 or train 2 is in operation and either train 3 or train 4 is in operation). The trains not in operation are isolated from the common headers and their associated Group 1 components are not in operation. Although two trains are not in operation, preventive maintenance may only be performed on one of these since the other one must remain available on standby to ensure that the single failure criteria can be met by the thermal barrier cooling function.

49 Following loss of either an operating CCWS pump or an operating ESWS pump, the CCWS and ESWS pumps on the standby train are automatically started if available. The standby train is also started on detection of low flow in the common header associated with the Group 2 components or high temperature on the operating CCWS train. Failure to switchover the common loads causes shutdown on one CVCS pump and two RCP pumps with consequential reactor trip. A leak that is sufficient to cause the water level in the tank associated with a CCWS train to fall despite automatic make-up results in automatic isolation of the header feeding the Group 4 components. If the leak persists, the other common header or the affected CCWS train is isolated.

50 In the original design, CCWS trains 1 and 2 were physically separated from CCWS trains 3 and 4. However, in developing a response to GDA issue **GI-UKEPR-FS-05**, EDF and AREVA have introduced a common header on the RCP thermal barriers under CMF#76 (Ref. 8). This modification is discussed further below.

51 The role of the ESWS is to cool the heat exchangers of the CCWS using seawater from the heat sink downstream from the Circulation Water Filtration System (CWFS). The ESWS has four trains that are independent and physically separated although there is a common header to allow re-supply of an ESWS train when the CWFS train on which it is connected is unavailable. The alignment is performed by realigning manual isolation valves on the suction header pipes. In normal operation trains 1 and 4 are supplied with filtered water from the side inlets of the CWFS which are fitted with chain filters while trains 2 and 3 are supplied from the central water inlets which are fitted with drum screens.

52 The safety classification of safety features on the CCWS and the ESWS will be determined during the site specific detailed design phase in response to Assessment Finding **AF-UKEPR-CC-05**. However, in Chapter 9.2 of the PCSR (Ref. 22), EDF and AREVA confirm that those features that are safety classified will need to meet the single failure criteria, have electrical supplies that are backed-up by diesels, and be seismically qualified. EDF and AREVA claim that the design of both systems has considered internal and external hazards.

53 Chapter 9.2 of the PCSR notes that through its direct link with the natural heat sink, the ESWS may be affected by external hazards affecting the CWFS. For the purposes of GDA the generic site assumption is that the heat sink function is performed by the sea which is effectively assumed to be infinite. Consideration of sites where the heat sink function is performed by a pipe running into a river estuary are outside the scope of GDA and will be assessed during the site specific detailed design phase.

Fault Sequence Analysis

54 EDF and AREVA have treated the three single failure faults listed above as design basis faults meeting the requirements of FA.4 and FA.5 although they have not formally allocated them as PCC events within the PCSR but as "specific studies". For this reason, I have raised Assessment Finding **AF-UKEPR-FS-90** for a future licensee to include these events within the design basis analysis of a site specific PCSR. Nevertheless, I recognise that the deterministic assessment performed does assume the most onerous single and the worst plant maintenance together with consequential LOOP following reactor trip so my judgement is that in practice the requirements of SAPs FA.6, EDR.2 and EDR.4 are being met although the radiological assessment still has to be presented. In addition to the deterministic assessment and as part of the site specific detailed design phase, it will also be necessary to model loss of essential support system faults within the PSA to confirm the balance of risk is ALARP when judged against SAPs T.8 and T.9. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-91** for a future licensee to perform such an assessment.

55 EDF and AREVA state (Ref. 16) that the initiating frequencies for these events are 0.2 per year for the break on a CCWS common header, 2×10^{-3} per year for the break on a CCWS train and 2×10^{-3} per year for the mechanical failure of a CCWS train. EDF and AREVA acknowledge that all three events are frequent faults. For this reason, they have performed a diversity analysis for common mode failure of frontline systems on demand in coincidence with these initiating events (Ref. 21) which I have assessed in my close-out report (Ref. 25) for Action 8 of GDA Issue **GI-UKEPR-FS-02** on functional diversity for frequent faults. In my report, I accept the adequacy of the safety case for the fault sequences that are presented but note that the scope of work is incomplete in that common mode failure of essential support systems when required on demand is not considered. I accept that such failures are likely to have a low conditional failure probability since essential support systems are continuously being tested in normal operation such that potential common mode failures are likely to be revealed and that the possibility for failure to start might be eliminated in circumstances where no system realignment is required. Nevertheless, there is a need to perform such an assessment, which is why I have raised Assessment Finding **AF-UKEPR-FS-45** in my close-out report (Ref. 25) for Action 8 of GDA issue **GI-UKEPR-FS-02**.

56 Returning to single failures, EDF and AREVA have performed a deterministic assessment (Refs 13 and 16) to establish the consequences of these single failure faults when coupled with the assumption of the most onerous single failure, the worst plant maintenance condition, and a consequential LOOP. In my judgement the approach is systematic and comprehensive. For each initiating fault, a series of tables are completed in which each permutation (excluding those cases discounted by symmetry arguments) of single failure and plant maintenance are analysed together with the assumption of LOOP. In addition, no claims are made on Class 2 systems such as the UDGs or the CHRS / UCWS diverse cooling chain or Class 3 systems such as the CVCS or SSSS.

57 The following single failures are considered:

- Failure of any one Emergency Diesel Generator (EDG) which when combined with LOOP results in the loss of one safeguard division.
- Failure of automatic CCWS train switchover.
- Failure of a CCWS common header.
- Failure of any one Extra Boration System (EBS) train which for the intact circuit cases can be onerous since the EBS is only a two train system.
- Failure of any one LHSI train which for LOCA cases can be onerous if only limited LHSI trains are operational due to the initiating event and the plant maintenance state considered.
- Failure of any one train of the safeguard building main HVAC system[1].
- Failure of any one train of the safeguard building diverse HVAC system[2].

58 The following plant maintenance states are considered:

- Any one EDG unavailable, which when combined with LOOP results in the loss of one safeguard division (although the electrical supplies for any EBS train or FPCS train will be cross connected from an adjacent division during maintenance);
- Any one train of the safeguard building main HVAC system unavailable (although the relevant train of the safeguard building diverse HVAC system will be used);

59 Some general characteristics can be noted. Depending upon which one of the two active CCWS trains is cooling the RCP thermal barriers at the time of the fault occurring, there is a 50% chance that CCWS cooling to the RCP thermal barriers will be lost for the case where the initiating event is due to a break. Since CVCS cooling and SSSS isolations are not claimed this is assumed to result in seal LOCAs on all four RCPs. In the alternate case, where the cooling to the RCP thermal barriers is maintained, two RCPs will be tripped due to loss of cooling of their motors and bearings causing a consequential reactor trip but with the primary circuit remaining intact.

60 The assumptions of single failure of one EDG or unavailability of one EDG when taken in coincidence with LOOP are quite onerous as an entire safeguard division is lost. Given that the initiating event generally removes a number of frontline systems in its associated safeguard division, assuming the loss of two EDGs due to single failure and plant maintenance removes a further two safeguard divisions largely leaving just one safeguard division to protect against the fault. Indeed, it will be seen in Section 4.6.2.1 below that the most onerous single failure initiating event is the loss of one 10 kV AC switchboard since this also completely removes one safeguard division such that of the four original safeguard divisions only one remains available. In contrast, the partial loss of cooling chain system events discussed here and the partial loss of safeguard building main HVAC system events discussed in Section 4.2.2.1 are slightly less onerous and so the assumption of only a single safeguard division being made available in the transient analysis studies is conservative for these two cases.

[1] EDF and AREVA call the ventilation trains of the safeguard building main HVAC system the DVL system while they call the chilled water trains of the safeguard building main HVAC system the DEL system.

[2] EDF and AREVA call the ventilation trains of the safeguard building diverse HVAC system the DVL_{new} system while they call the chilled water trains of the safeguard building diverse HVAC system the DEL_{new} system.

61 Another feature is that for intact circuit sequences, one of the challenges is to ensure the long term control of reactivity since potentially both EBS trains can be lost. This aspect is discussed further below in my assessment of the proposed design change presented in CMF#75 (Ref. 8).

62 EDF and AREVA have specific PCC analysis rules for the design basis assessment of the spent fuel pool. These exclude consideration of single failure occurring with LOOP unless the component on which the single failure occurs is not seismically qualified (Ref. 13). While I can see the logic for this approach, when applied to a frontline system such as the FPCS where loss of the system will not result in a reactor trip and so the conditional probability for LOOP will be low, it is not clear these rules remain valid when it is an essential support system that initiates the loss of cooling fault as this can also result in a reactor trip. However, I note that as a result of GDA issue **GI-UKEPR-FS-03** (Ref. 26) that the spent fuel make-up system is being upgraded to Class 1 and so provides a diverse means of ensuring spent fuel pool cooling in addition to the pre-existing capability provided by the main FPCS trains which under CMF#38 are being upgraded to Class 1 and the diverse 3rd FPCS train which under CMF#36 is being upgraded to Class 2. I have raised Assessment Finding **AF-UKEPR-FS-92** for a future licensee to justify the design basis analysis rules applied to the analysis of loss of essential support system faults affecting the FPCS and to confirm that adequate protection is provided.

63 In developing the safety case EDF and AREVA have proactively identified the need for a number of design changes to ensure compliance with the design basis analysis rules. These design changes are generally associated with upgrading the safety classification of the C&I systems that are claimed to actuate engineered safeguards such as the switchover or the isolation of safety trains and the tripping of the RCPs. However they have also identified the need to provide additional functionality to improve protection against these faults. The design changes identified are presented in a series of CMFs that are discussed in the following paragraphs. Progress with these modifications will be monitored by ONR during the site specific detailed design phase through the generic cross cutting Assessment Finding **AF-UKEPR-CC-01** (Ref. 27) which requires a future licensee to implement any design changes identified during GDA.

64 CMF#39 (Ref. 8) covers the following design change:

- To provide a means of realigning an EFWS pump discharge from the Main Control Room (MCR). This is to protect against the situation where one or more SGs have been isolated (Steam Generator Tube Rupture (SGTR) faults with a plant maintenance of one EFWS pump can also cause this situation) and the RCP pumps have been tripped. Since the SGs are not removing heat, natural circulation flow in the affected loops can stop. If these loops are associated with one EBS train and the other EBS train is subject to a single failure then maintaining the core sub-critical can be challenged. This is especially the case when only one safeguard division is available as considered here. The intention is to manually realign the operational EFWS pump on the common discharge header to feed an alternate Steam Generator (SG) to prevent it from drying out. To improve both the reliability and the response time, EDF and AREVA are proposing a modification to allow the operation to be performed from the MCR rather than local to plant. The signal will also be upgraded to Class 1. I note that the proposal will also reduce concerns over a potential thermal shock associated with re-feeding a dried-out SG.

65 CMF#42 covers the following three design changes:

- The automatic switchover from the duty CCWS train to the standby CCWS train will be upgraded to Class 1. This will require the use of Class 1 redundant sensors which will be allocated on to the same TXS platform technology that is also used for the reactor protection system (PS). In addition, as frequent faults are being protected against, a diverse signal will be introduced on the Safety Automation System (SAS) subject to a detailed ALARP review during the site specific detailed design phase. EDF and AREVA claim that it is not ALARP to provide redundant mechanical valves for the switchover due to the impact on plant layout. However, it not clear whether redundant mechanical valves are actually required to meet the single failure criteria at the functional level since even if the train realignment fails there are still the other two trains of the CCWS available to perform the safety function. This needs to be confirmed since it is my expectation that a Class 1 system on a new reactor design would meet the single failure requirements of SAP EDR.4. For this reason, I am raising Assessment Finding **AF-UKEPR-FS-93** for a future licensee to confirm that the single failure criterion is met with the proposed design.
- The automatic isolation of the CCWS common header will be upgraded to Class 1. This will require the use of Class 1 redundant sensors which will be allocated to a TXS platform. In addition, as frequent faults are being protected against a diverse signal will be introduced on the SAS subject to a detailed ALARP review during the site specific detailed design phase. EDF and AREVA claim that it is not ALARP to provide redundant mechanical valves for the isolation due to the impact on plant layout. However, it not clear whether redundant mechanical valves are actually required to meet the single failure criteria at the functional level since even if an isolation valve fails there are still two other trains of the CCWS available to perform the safety function and so this needs to be confirmed. I consider that Assessment Finding **AF-UKEPR-FS-93** is equally applicable to this case as well.
- The automatic trip of an RCP pump on loss of thermal barrier cooling or loss of motor cooling will be upgraded to Class 1. This will require the use of Class 1 redundant and diverse sensors based upon temperature and flow rate measurements which will be allocated to a TXS platform. It is proposed to provide double breakers on the RCP pump subject to a detailed ALARP review during the site specific detailed design phase. In addition, as frequent faults are being protected against the feasibility of providing a diverse signal on the SAS or Non-Computer based Safety System (NCSS) will also be subject to a detailed ALARP review during the site specific detailed design phase.

66 CMF#75 (Ref. 8) proposes a number of ALARP studies to improve the capability of the UK EPR™ to reach the safe shutdown state. The following proposals are to be developed further during the site specific detailed design phase:

- The current design of the UK EPR™ requires that two neighbouring C&I divisions should be available in order to reach the safe shutdown state by allowing the operator in the MCR to open the SG Main Steam Relief Trains (MSRT) to enable cooldown of the primary circuit as explained in their response to TQ-EPR-1621 (Refs 9, 15 and 28). EDF and AREVA acknowledge (Ref. 16) that feasible alternate design options to the control logic of the hydraulic system have been implemented on other EPR™ projects which open the MSRTs even when two neighbouring C&I divisions are not available which avoid introducing weaknesses into the design with regard to the risk of spurious opening of the MSRT during normal operation.

- Given that the EBS is only a two train system, loss of three safeguard divisions can result in the loss of the long term control of reactivity safety function when the primary circuit remains intact. EDF and AREVA are considering recovery using electrical inter-connections between neighbouring divisions (1& 2) and (3 & 4) although ensuring HVAC cooling of the EBS pump rooms also needs to be considered. Alternatively, the safeguard building new diverse HVAC system proposed under CMF#77 discussed in Section 4.2.2.1 below or start-up of an Ultimate Diesel Generator (UDG) to re-supply electrical power to either Division 1 or 4 may be claimed.

67 Although this modification, like all the other CMFs, is covered by the generic Assessment Finding **AF-UKEPR-CC-01** (Ref. 27), it is very preliminary in nature. I have therefore raised Assessment Finding **AF-UKEPR-FS-94** for a future licensee to further develop CMF#75 into a more specific proposal. Given the potential implications for plant layout of these changes it is essential in my judgement that the analysis and design work is substantially completed early in the site specific detailed design phase and prior to the pouring of Nuclear Island safety-related concrete.

68 CMF#76 (Ref. 8) proposes a design change to improve protection against loss of a single CCWS train during maintenance.

- EDF and AREVA are proposing to include an additional common header on the RCP thermal barrier cooling lines such that one CCWS train can cool the RCP thermal barriers on all four RCP seals. The proposal also raises the safety classification of the RCP thermal barrier cooling lines to Class 1. The design intent is to reduce the likelihood of loss of RCP thermal barrier cooling occurring when performing periodic maintenance on one of the CCWS trains. In the original design, where pairs of CCWS trains are totally segregated from each other, the RCP thermal barriers of two pump seals are vulnerable to a single failure on the duty CCWS train whenever the standby CCWS train is unavailable due to maintenance. With the revised design the common header will be aligned so all the thermal barriers take their cooling from the CCWS pair not associated with plant maintenance activities so reducing vulnerability to the single failure. The disadvantage with this proposal is that it makes all four RCP thermal barriers vulnerable to a single break on this common header. It also potentially cuts across the segregation of the CCWS train pairs if the correct isolations (double isolations are provided on each CCWS train) are not performed. EDF and AREVA claim to have considered providing automatic or manual double isolations on the common header to restore the original design intent but state that these options are complex and could not detect a break quickly enough to be effective. However, no discussion is given of the possibility of isolating the common header for the majority of the time when maintenance is not being performed on one of the CCWS trains. EDF and AREVA state (Ref. 16) that the basic solution was proposed based upon studies prepared for Flamanville 3 (FA3). These studies have not been shared with ONR and so I am raising Assessment Finding **AF-UKEPR-FS-95** for a future licensee to provide further justification that the proposed design change is ALARP.

69 As a result of the fault sequence analysis, which assumes the above modifications are in place, EDF and AREVA conclude (Refs 13 and 16) that for the reactor the following new design basis faults bound the fault sequences that have been discussed above:

- Two tripped RCPs with loss of three safeguard divisions.
- Four RCP seal LOCAs with loss of three safeguard divisions.

70 I agree with this conclusion and consider it to be conservative for the case of partial loss of cooling chain faults providing the proposed modifications discussed above and covered by Assessment Findings **AF-UKEPR-CC-01** and **AF-UKEPR-FS-93** to **AF-UKEPR-FS-95** are fully implemented. I therefore judged that the functional analysis performed by EDF and AREVA to identify these sequences meets the requirements of SAPs FA.6, EDR.2 and EDR.4.

Methods and Assumptions

71 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling these two design basis fault sequences, EDF and AREVA have made the following assumptions (Ref. 15) to ensure a robust and conservative assessment.

- The initial and boundary conditions are penalised to be consistent with PCC analysis rules including conservative estimates for decay heat.
- 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.

72 The EDF and AREVA analyses use the CATHARE computer code to model the two design basis faults. The assessment of the CATHARE code against SAPs FA.17 to FA.22 is reported in the GDA Step 4 Fault Studies Assessment of the UK EPR™ (Ref. 2). This concludes that 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 alternate codes such that it meets the requirements of SAPs FA.17 to FA.22.

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

Transient Analysis

74 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. To confirm that this objective has been achieved, the results of design basis analysis of EDF and AREVA need to be assessed. The following paragraphs present my assessment of the results of the transient studies (Ref. 15) for the seal LOCA on four RCPs fault with only one division of safeguard equipment available and the two RCP trip fault with only one division safeguard equipment available.

75 The results of the EDF and AREVA analysis for the seal LOCA fault are summarised in Figures 4 and 9 of the transient analysis report (Ref. 15) which present the upper plenum level transient for reaching the controlled state and the safe shutdown state respectively. These results demonstrate that the core remains covered throughout the transient such that fuel damage will be avoided. It should be noted that although three safeguard divisions are assumed to be lost the automatic and manual cooldown function is still claimed to be available on three divisions during the first 6000 seconds of the transient on grounds that the battery backed-up C&I controlling the MSRT valves remains available for

the first two hours. This ensures that the primary pressure is lowered sufficiently for the MHSI injection flowrate to match the break flowrate.

76 The main item of interest is that, initially only one SG is fed. This SG is overfed such that its level starts to rise since the heat removal capacity is limited by the surface area of the SG tube sheets during natural circulation conditions. In contrast, the other SGs are not fed and gradually empty reaching the relevant isolation level after 4000 seconds. EDF and AREVA wish to claim the operator to realign the operating EFWS pump to feed a second SG in less than one hour, which is why they are proposing CMF#39 discussed above to allow realignment of the EFWS from the MCR using a Class 1 system. The proposals under CMF#75 are also needed after two hours to allow more than one MSRT to be claimed. The controlled state is reached when two SGs are fed by one EFWS pump and two MSRT evacuate heat and one MHSI pump compensates for the break. The boration function is achieved by the safety injection systems taking supplies from the IRWST. In the longer term the operator will switch from MHSI to LHSI with cooling to the IRWST provided by the one remaining CCWS train. Only if the saturation margin criterion and the P14 interlock set-point for Residual Heat Removal (RHR) connection can be met will the operator subsequently switch off the one remaining LHSI pump and switch it to RHR mode of injection (Ref. 28).

77 In the case of the two RCP trip fault, EDF and AREVA argue (Ref. 15) that the initial pre-trip transient is bounded by the LOOP transient modelled in the PCSR which results in the trip of all four RCPs, and which demonstrates that departure from nucleate boiling (DNB) will be avoided. I accept this argument. The results of the EDF and AREVA analysis for the RCP trip fault are summarised in Figure 13 of the transient analysis report (Ref. 15) which presents the primary pressure transient while reaching the controlled state. After approximately 4000 seconds the lift pressure of the Pressuriser Safety Valves (PSVs) is reached. This is because initially only one SG is fed. As with the seal LOCA case, this SG is overfed such that its level starts to rise since the heat removal capacity is limited by the surface area of the SG tube sheets during natural circulation conditions. In contrast, the other SGs are not fed and gradually empty reaching the relevant isolation level between 3000 and 4200 seconds. It is undesirable to allow the PSVs to lift in water solid conditions which is why EDF and AREVA wish to claim the operator to realign the operating EFWS pump to feed a second SG in less than one hour under the CMF#39 proposal discussed above to allow realignment of the EFWS from the MCR using a Class 1 system. The proposals under CMF#75 are also needed after two hours to allow more than one MSRT to be claimed and to ensure the availability of the EBS to provide for the long term control of reactivity.

78 In summary, on the basis of the analysis presented and subject to satisfactory completion of these modifications under the generic Assessment Finding **AF-UKEPR-CC-01** (Ref. 27), I am satisfied that the requirements of SAP FA.7 have been met for these two transients.

4.1.2.2 Total Loss of a Cooling Chain System

System Description of the Diverse Cooling Chain Systems

79 Before reviewing the fault sequence analysis it is worth reviewing the system designs for the CHRS and the UCWS.

80 Chapter 6.2 of the PCSR (Ref. 23) states that the role of the CHRS is:

- To limit containment pressure in severe accident conditions.

- To provide cooling to the 3rd train of the FPCS.
- To provide cooling to the IRWST following a SBLOCA with total loss of LHSI.
- To provide cooling to the IRWST following the total loss of cooling chain systems in state D.

81 As result of the functional analysis performed in response to GDA issue **GI-UKEPR-FS-05** (Ref. 17) the role of the CHRS has been increased to the following:

- To provide cooling to the IRWST following the total loss of cooling chain systems in states A, C & D.

82 The CHRS is a two train system that is supplied with electrical power from Divisions 1 and 4 of the 690 V Alternating Current (AC) essential electrical system. Each train of the CHRS is cooled via an intermediate CHRS train that is in turn cooled by a train of the UCWS. Train 1 of the intermediate CHRS also cools the 3rd train of the FPCS. Each CHRS train takes its suction from the IRWST using either the sump filter on the Safety Injection System (SIS) train associated with the CHRS train or, via a cross connection, the sump filter of the neighbouring SIS train. Each CHRS train can be used for the containment spray function, for back flushing to clean debris from either of the two sump filters that it can take suction, or to cool the corium spreading compartment in severe accident conditions. In Chapter 6.2 of the PCSR (Ref. 23), EDF and AREVA claim that the CHRS will be tested periodically to confirm its availability.

83 The role of the UCWS is to cool the heat exchangers of the intermediate CHRS which cools the front line CHRS and (for train 1 only) the 3rd train of the FPCS using seawater from the heat sink downstream from the CWFS. The UCWS has two trains that are independent and physically separated. The suction of UCWS pumps can be aligned to a chain filter or a drum screen using a header pipe.

84 EDF and AREVA claim that diverse supplies can be provided in some situations associated with loss of the pumping station, since each UCWS pump may be supplied with water taken from the discharge culvert via diverse piping. The UCWS discharge is redirected to the intake channel. These realignments are performed manually on detection of large pressure drops across the filters protecting the UCWS pump. EDF and AREVA argue that the time taken to perform this action is compatible with the grace period calculated for these events. It also implies that the diverse suction piping is sized for shutdown states E and F when decay heat levels will be lower. However, this may still be adequate for the diverse role being assessed here providing sufficient decay heat is removed by the Steam Generators (SGs) using the EFWS. This aspect is discussed further below in the section on transient analysis.

85 In Chapter 9.2 of the PCSR (Ref. 22), EDF and AREVA state that the CHRS comprises two 50% trains which are necessary to provide cooling for the first 15 days following a severe accident. Beyond this time one train is sufficient. This does not however correspond to the situation considered here where a component of the decay heat can be removed from the core using the EFWS. Again, this aspect is discussed further below in the section on transient analysis.

86 The safety classification of safety features on the CHRS and the UCWS will be determined during the site specific detailed design phase in response to Assessment Finding **AF-UKEPR-CC-05** but given they are being claimed as diverse safety systems my expectation is that they would attract a safety classification of at least Class 2 consistent with the commitment made by EDF and AREVA in CMF#36 (Ref. 8). In Chapter 6.2 of the PCSR (Ref. 23) and Chapter 9.2 of the PCSR (Ref. 22), EDF and

AREVA confirm that these systems are provided with electrical supplies that are backed-up by the EDGs and the UDGs. EDF and AREVA argue that the design of both systems has considered internal and external hazards as appropriate on a case by case basis. Nevertheless, the PCSR notes that the CHRS and UCWS will be seismically qualified apart from the diverse suction function of the UCWS. This may be an aspect of the design that ONR will choose to explore further during the site specific detailed design phase.

Fault Sequence Analysis

87 The PCC analysis rules of EDF and AREVA do not apply to faults caused by a common mode failure. Nevertheless, EDF and AREVA acknowledge that such events occur with a frequency of about 10^{-5} per year (Ref. 17) and so have performed a design basis analysis for this fault consistent with UK practice in which additional failures are considered if the resultant sequence frequency is still greater than 10^{-7} per year (Ref. 7). In practice, this has required EDF and AREVA to consider an additional plant maintenance state but not an additional single failure or consequential LOOP. In my judgement, this approach meets the requirements of SAPs FA.4 and FA.5. It should be noted that meeting this requirement demonstrates additional margin within the design on those occasions when plant is not in a maintenance condition since it will then generally be tolerant to an additional single failure as well as the common mode failure.

88 In developing the safety case EDF and AREVA have proactively identified the need for a number of design changes (Ref. 17). These are generally associated with upgrading the safety classification of the C&I systems that are claimed to actuate engineered safeguards such as the actuation of the CHRS. These design changes are covered by CMF#79 (Ref. 8) except where they are already covered by the design changes under CMF#41 (discussed in Section 4.2.2.1 below) and CMF#42 (discussed in Section 4.1.2.1 above).

89 CMF#79 (Refs 8 and 17) covers upgrading to Class 1 if ALARP of the following automatic actuations:

- LHSI pumps in RHR mode trip on high CCWS temperature or low CCWS flowrate.
- Safety injection signal to start LHSI pumps in reduced flowrate mode on low loop level.
- Upgrade of the associated sensors.
- Upgrade of the CHRS / UCWS pump and motor electrical and C&I requirements to Class 1.

90 CMF#79 (Refs 8 and 17) also covers upgrading to Class 1 the following manual actuations:

- Cooldown with MSRT.
- Accumulator isolation.
- Opening of the feed and bleed valves.
- Actuation of CHRS.
- Opening of purification line valves at the bottom of the reactor pool.
- SG level control.

91 However, the design changes proposed under CMF#79 (Ref. 8) are associated with a number of caveats and subject to further ALARP assessments (Refs. 8 and 16) during the site specific detailed design phase. For this reason, in order to reduce the regulatory uncertainty associated with these design proposals, I have raised Assessment Finding **AF-UKEPR-FS-96** for a future licensee to complete these assessments. Given the potential impact of the design changes on plant layout in my judgement it is essential that this analysis and design work is substantially completed early in the site specific detailed design phase and prior to the pouring of Nuclear Island safety-related concrete.

92 As result of the fault sequence analysis, which assumes the above modifications are in place, EDF and AREVA conclude (Refs 16 and 17) that depending on the reactor state, the following new design basis faults are needed to bound the fault sequences that have been identified from the above analysis:

- Total of loss of CCWS / ESWS in plant state A with one CHRS / UCWS train unavailable due to maintenance.
- Total of loss of CCWS / ESWS in plant state Cb2.
- Total of loss of CCWS / ESWS in plant states Cb3 and D.

93 Total loss of cooling chain in state A (at power) is assumed to result in the trip of the RCPs. It also results in seal LOCAs on all four RCPs since the SSSS cannot be claimed for design basis events. Loss of cooling chain also results in the consequential loss of all MHSI pumps and the two LHSI pumps on Divisions 2 and 3. In addition, the loss of cooling chain will result in the loss of the safeguard building main HVAC in Divisions 2 and 3 which rely upon chilled water cooling. This has the potential to result in the total loss of the safeguard equipment in Divisions 2 and 3 due to consequential failure of C&I and electrical equipment in these divisions. However, EDF and AREVA argue that the provision of the safeguard building new diverse HVAC system discussed further in Section 4.2.2.1 below will protect against these failures taking into account the sequence frequencies and the conditional probability for the external air temperature being above 25°C. In summary, the fault sequence results in two LHSI pumps being available to protect against the seal LOCA fault with IRWST cooling provided by one train of CHRS / UCWS together with four EFWS pumps which are claimed to remove the majority of the decay heat. The transient analysis studies for this case are discussed below.

94 Total loss of cooling chain in state Cb2 (reactor shutdown with pressuriser vent open) is assumed to result in the overheating of the LHSI pumps in RHR mode or a reduction in CCWS flow causing the LHSI pumps in RHR mode to be tripped on protection signals. As cooling is lost the primary coolant temperatures increase until saturation conditions are reached and primary inventory reduces triggering safety injection. All four MHSI pumps and the LHSI pumps in Divisions 2 and 3 are again assumed to fail due to total loss of the cooling chain fault. Only LHSI pumps in Divisions 1 and 4 remain available. As the reactor is shutdown the SGs may or may not be available. If available they can be used to extract heat with the LHSI providing a make-up capability. Alternatively, a feed and bleed operation can be initiated in order to allow sufficient safety injection from the LHSI. In order to ensure a sufficient supply of coolant is provided to the LHSI pumps the purification line valves of the FPCS at the bottom of the reactor pool are claimed to be manually opened to allow the recirculation of coolant from the reactor pool to the IRWST. The heat removal function is performed by two trains of the CHRS / UCWS. Since both trains have to be claimed plant maintenance is not allowed on the CHRS / UCWS during shutdown operations. The transient analysis studies for this case are also discussed below.

95 Total loss of cooling chain in states Cb3 or D (reactor shutdown, vessel open, with ¾ loop operation) is also assumed to result in the overheating of the LHSI pumps in RHR mode or a reduction in CCWS flow causing the LHSI pumps in RHR mode to be tripped on protection signals. The resultant fault sequence is similar to the case for state Cb2 apart from the fact the SGs will definitely not be available and bleed and feed operations will not be required since the reactor is already depressurised. The transient analysis studies for this case are also discussed below. Note that EDF and AREVA claim that state E is bounded by state D while in state F the fuel is unloaded from the reactor.

96 Total loss of cooling chain also affects the cooling of the spent fuel pool. EDF and AREVA acknowledge (Ref. 16) that all three FPCS trains could be lost after taking into account the at power plant maintenance states allowed on the intermediate CHRS and UCWS trains that cool the 3rd train of the FPCS. EDF and AREVA argue that in plant state A the spent fuel pool will take 14 hours to start to boil and 30 hours to start to uncover fuel and that one train of the spent fuel pool make-up system, which has been upgraded to Class 1 in response to GDA issue **GI-UKEPR-FS-03** (Ref. 26), has sufficient capacity to provide adequate cooling.

97 Subject to the claimed modifications being satisfactorily implemented, I agree that these design basis fault sequences meet the requirements of SAPs FA.6, and EDR.2 to EDR.4 and in the case of reactor faults need to be studied using transient analysis.

Methods and Assumptions

98 SAP FA.7 requires that the analysis of design basis fault sequences should be performed on a conservative basis. In modelling these fault sequences, EDF and AREVA have made use of pre-existing Risk Reduction Category A (RRC-A) analysis reported in Chapter 16.1 or performed new analyses for FA3. The latter have not been assessed by ONR. EDF and AREVA acknowledge that such analyses does not provide the bounding assessment normally performed for design basis faults as would be the expectation to meet the requirements of SAP FA.7 and confirm that such analyses will be performed during the site specific detailed design phase.

Transient Analysis

99 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. To confirm that this objective has been achieved, the results of design basis analysis of EDF and AREVA need to be assessed. The following paragraphs present my assessment of those cases where transient analysis studies are available to support the functional analysis performed by EDF and AREVA (Ref. 17) of the total loss of cooling chain fault sequences in plant states A, C & D as discussed above.

100 For the case of total loss of cooling chain in plant state A, EDF and AREVA state (Ref. 17) that the pressure and temperature qualification profiles for the containment are respected and that the maximum IRWST temperature does not exceed 110°C during the first 24 hours after the initiating event and 100°C after 24 hours based upon calculations performed for FA3 for the event of station blackout with RCP seal break in state A. EDF and AREVA argue that the consequences for a total loss of coolant chain fault in state A, in terms of containment pressure and temperature and IRWST temperature, will be bounded by the Station Blackout Sequence (SBO). Given that only two SGs will be fed in

the station blackout sequence compared with the four SGs fed in the total loss of cooling chain fault sequence and there will be a delay before the safeguard systems start due to the operator having to start-up the UDGs, I accept this argument. However, I have not assessed this SBO analysis as it has not been presented to ONR, although I do discuss this important sequence further in Section 4.6.2.2 below. EDF and AREVA acknowledge there is a need to provide UK EPR™ specific calculations during the site specific detailed design phase to confirm that the CHRS is adequately sized. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-97** for a future licensee to perform this analysis. Given the potential implications for plant layout, in my judgement it is essential that this analysis and design work is substantially completed during the early stages of the site specific detailed design phase and prior to the pouring of Nuclear Island safety-related concrete.

101 Nevertheless, the loss of cooling chain fault in plant state A is considered as a RRC-A sequence in Section 3.5 of Chapter 16.1 of the PCSR (Ref. 23). No transient analysis is presented but the case is argued to be bounded by two other RRC-A sequences for which transient analysis studies are available. EDF and AREVA argue that the secondary side systems such as the EFWS and MSRT are unaffected by the event and so core heat removal is assured by the secondary side as long as the primary inventory is sufficiently high to maintain primary flow. They argue that the following accident scenario would occur.

102 Following the total loss of cooling chain, the accident is detected by the reactor PS due to the tripping of the RCPs on loss of seal injection and thermal barrier and the corresponding reactor trip on low pump speed. The coast down occurs over five minutes and then natural circulation ensures decay heat removal from the core. On the secondary side heat removal is through the main steam bypass or the MSRT at pressure levels above 90 bar and temperatures greater than 300°C. Given that it is a loss of cooling chain fault that is being considered, EDF and AREVA acknowledge that the combination of high pressure (155 bar) and temperature (300°C) will cause the RCP shaft seals and the SSSS to fail.

103 EDF and AREVA claim it is conservative to assume that the failure of the RCP seals with no closure of leak-off lines leads to a maximum break flow of about 28 kg/s per RCP at the initial operating pressure giving a total initial break flow from all four pumps of 112 kg/s. This is about half the value considered for the frequent SBLOCA based upon a bounding break size of 20 cm^2. EDF and AREVA therefore argue that the transient analysis studies for the RRC-A sequence SBLOCA without MHSI bounds this case since the break size is practically double compared with the current case. Using the SBLOCA transient studies they argue that after about 5 minutes the safety injection will be reached on low pressuriser pressure which automatically actuates secondary side partial cooldown to about 55 bar. Both MHSI and LHSI pumps start operating but, with the exception of the two LHSI pumps in Division 1 and 4, which have the CHRS / UCWS diverse cooling chain, they will fail with time because of the total loss of cooling chain. Core heat-up is estimated to occur after about 2 to 2.5 hours since the primary pressure is too high for the LHSI to inject unless operator action is taken to mitigate the accident by depressurising the primary circuit.

104 The operator initiates fast cooldown by fully opening the MSRTs to depressurise the secondary side such that the primary pressure drops below the LHSI pump head of 20 bar. The emergency operating procedures require the operator to do this whenever there is a safety injection signal and no MHSI flow. During the depressurisation the accumulators automatically inject at 45 bar such that the heat up, which is very limited,

will stop. The accumulators also inject sufficient boron to ensure the long term control of reactivity. Long term make-up is ensured by the two LHSI pumps since only one LHSI is required to compensate for the break flow and long term decay heat removal is ensured by the SG using the EFWS and MSRTs that are not affected by the initiating event such that core cooling degradation never occurs. By comparison with the transient studies for SBLOCA without MHSI, which were assessed during Step 4 of GDA (Ref. 2), the current transient case is bounded because the break size is smaller and the MHSI pumps will operate in practice for about the first 15 minutes before they fail.

105 EDF and AREVA claim that the containment pressure and IRWST temperature build-up during this accident scenario will remain well below the relevant design safety limits and are not significant arguing that the case is bounded by the RRC-A sequence SBLOCA with failure of all LHSI pumps presented in Section 3.8 of Chapter 16.1 of the PCSR (Ref. 23). This is because the break size is smaller such that the containment pressure build up and the heat load for the IRWST are bounded given that there is no cooling from the CHRS for the first few hours. These studies predict that the peak containment pressure and maximum IRWST water temperature are 2 bar and 90°C respectively. This latter sequence is discussed in the close out report for Action 9 of GDA issue **GI-UKEPR-FS-02** (Ref. 25).

106 The SBLOCA with failure of all LHSI pumps presented in Section 3.8 of Chapter 16.1 of the PCSR deserves comment in its own right since it refers to an earlier study in Appendix 16.B of the PCSR (Ref. 23). This was performed for a previous 4900 MW design of the EPR™ and is based upon a different design for the CHRS which directly cools the IRWST using a heat exchanger rather than using the containment spray system to cool the IRWST. The latter will be less effective since some cooling capacity is dissipated cooling hot structures within the containment. As this is an RRC-A analysis, EDF and AREVA also discount plant maintenance and so claim both trains of the CHRS. The analysis also models the main steam bypass system and start-standby feed system to cool the secondary side rather than the MSRT and EFWS that would normally be expected to be claimed for design basis sequences. However, this may not be significant since all four trains of the MSRT / EFWS would be available and in any case the MSRTs are capable of blowing down the SGs faster than the main steam by-pass system. Best estimate decay heat levels are also assumed in the 4900 MW analysis. EDF and AREVA judge that the higher decay heat for the 4900 MW design compared with the 4500 MW UK EPR™ design and a conservatively low IRWST water inventory will cover any uncertainty in the modelling of this sequence including the differences in the design of the CHRS. The increase in automatic partial cooldown rate implemented under CMF#10 during GDA Step 4 (Ref. 2) will also be beneficial.

107 EDF and AREVA quote (Ref. 23) an energy balance at 4 hours into the transient which shows that the total heat removed from the reactor and structures is 45.7 MW of which 32.7 MW is being removed by the SGs and 13.0 MW is being removed by the break to the containment and IRWST. The 4900 MW analysis quotes the capacity of one CHRS heat exchanger as 13 MW at an inlet temperature of 94°C implying that one CHRS trains is just about functionally capable of protecting against the fault by providing adequate cooling to the IRWST to ensure that the MHSI pumps continue to operate without tripping.

108 It is helpful to compare the heat removal requirements of the one CHRS / UCWS train with that of one CCWS / ESWS train. The CCWS system design manual (Ref. 29) sizes the CCWS / ESWS heat exchangers on the four trains so as to remove 33 MW, 36 MW, 35 MW and 33 MW respectively when in RHR mode with the Reactor Coolant System (RCS) temperature at 100°C. This sizing is chosen so as to be able to cool the reactor

down from 120°C to 55°C in six hours. In the calculation, trains 2 and 3 are shown to remove slightly more heat since they are aligned to cool the FPCS. In practice, this capability means that in accident conditions one CCWS train is able to remove 71 MW when in RHR mode with the RCS temperature at 180°C.

109 In contrast, the CHRS system design manual (Ref. 30) and Chapter 6.2 of the PCSR (Ref. 23) confirm that one CHRS train is sized to remove 11.5 MW with the IRWST temperature at 94°C (quoted for Risk Reduction Category B (RRC-B) severe accident conditions) and 18 MW with the IRWST temperature at 120°C (quoted for the RRC-A sequence SBLOCA with loss of LHSI). The lower heat removal capacity of the current CHRS design means that potentially both trains of the CHRS need to be available. The CHRS system design manual (Ref. 30) states that the RRC-A sequence covering total loss of cooling chain in state D is less onerous although no figures are provided to quantify this claim.

110 The sizing requirements (Ref. 30) for the intermediate CHRS heat exchanger and the UCWS are greater since the design of the two redundant trains is identical even though one of them has to be sized to remove 20 MW from the 3rd train of the FPCS with an inlet temperature of only 95°C. This implies that there is scope for increasing the heat removal capacity of the frontline CHRS trains without affecting the sizing of the downstream cooling systems. Given that it is proposed to allow plant maintenance on one train of the CHRS when the reactor is at power, with the current design of the CHRS there may potentially be times when it will not be functionally capable of fulfilling its role as part of the diverse cooling chain for the frequent SBLOCA fault coupled with common mode failure of the LHSI due to the marginal reduction in its sizing.

111 It is not clear that this is adequate or ALARP. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-98** for a future licensee to perform a design basis assessment for the frequent SBLOCA fault with failure of the LHSI to demonstrate that a single train of the current CHRS design is capable of providing adequate cooling to the IRWST or explore the feasibility of increasing the heat removal capacity of the CHRS to ensure it can do so prior to the pouring of Nuclear Island safety-related concrete. Note that the case of the SBO sequence in plant state A with failure of SSSS, which also needs to claim the CHRS / UCWS cooling chain and is probably more limiting, is considered in Section 4.6.2.2 below.

112 It is worth noting that the loss of cooling chain fault in plant state A is also considered as a RRC-A sequence in Section 3.12 of Chapter 16.1 of the PCSR (Ref. 23) for the case in which the SSSS does not fail. This is used to demonstrate that 100 hours are available for re-supplying the EFWS tanks using the fire fighting water system to avoid SG dry-out following loss of cooling chain or ultimate heat sink.

113 No discussion is provided on whether the UCWS diverse suction piping is adequately sized for the loss of cooling chain fault. Given that the initiating event could be due to the total loss of ultimate heat sink consideration needs to be given to the situation where the UCWS has to be switched to this diverse intake. Confirmation is needed that a single train of the diverse intake is sufficiently sized to provide adequate cooling when only a single CHRS / UCWS train is available for the total loss of cooling chain fault occurring in plant state A. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-99**, for a future licensee to confirm the adequacy of this sizing.

114 For the total loss of cooling chain fault in plant states C and D no transient analysis results are available. EDF and AREVA state (Ref. 17) that the pressure and temperature qualification profiles for the containment are respected and that the maximum IRWST

temperature does not exceed 110°C during the first 24 hours after the initiating event and 100°C after 24 hours based upon calculations performed for FA3 for plant state D. Given that the reactor is already shutdown, depressurised and cooled before the fault occurs and given that two CHRS trains are available for decay heat removal this result appears reasonable. Nevertheless, EDF and AREVA acknowledge there is a need to provide UK EPR™ specific calculations during the site specific detailed design phase. This will need to confirm the grace period available for the operator to open the purification line valves on the FPCS and that the CHRS is adequately sized. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-100** for a future licensee to perform this analysis.

115 Finally, it is worth placing the total loss of cooling chain fault into context. The analysis performed by EDF and AREVA in response to GDA Issue **GI-UKEPR-CC-03** on the lessons learnt from Fukushima studies the complete loss of ultimate heat sink (Ref. 31). In this analysis both the CCWS / ESWS cooling chain and the CHRS / UCWS cooling chain are assumed to be lost due to the initiating event. These best estimate studies illustrate the grace time available following total loss of ultimate heat sink in plant state A. The design basis analysis discussed above assumes that the SSSS fails to operate resulting in seal LOCA. In practice the SSSS is designed to work automatically and it is claimed (Ref. 31) that it would retain its structural integrity for 24 hours. In this situation assuming EFWS is available and the operator has already performed a cooldown on the primary circuit using the MSRTs, EDF and AREVA estimate (Ref. 31) that significant loss of inventory would not occur until approximately five days after the initiating event. The operator is then claimed to start-up the LHSI pumps in Divisions 1 and 4 taking suction from the IRWST. This could continue until the IRWST temperature reaches 120°C at which point the LHSI would cease to operate and core heat up would commence. I have not assessed the calculations, arguments and evidence underpinning these claims but I do accept that there would be a considerable grace period particularly if an external connection is made to the containment spray system to enable water injection into the containment using a mobile pump, since this would prolong the period before LHSI failure occurs.

116 In summary, on the basis of the analysis presented and subject to satisfactory completion of the proposed modifications under generic Assessment Finding **AF-UKEPR-CC-01** and Assessment Finding **AF-UKEPR-FS-96**, I am satisfied that sufficient progress has been made to give me confidence that the requirements of SAP FA.7 can be met for the loss of cooling chain transient in states A, C and D for the purposes of GDA recognising that additional confirmatory transient analysis, being provided in response to Assessment Findings **AF-UKEPR-FS-97** to **AF-UKEPR-FS-100**, will become available prior to the pouring of Nuclear Island safety-related concrete.

4.1.3 Findings

117 Following my assessment of the EDF and AREVA submissions, I am satisfied that sufficient progress has been made for the purposes of GDA such that GDA issue **GI-UKEPR-FS-05** can be closed with regard to loss of cooling chain faults. A number of Assessment Findings **AF-UKEPR-FS-90** to **AF-UKEPR-FS-100** have been raised for a future licensee to complete the work during the site specific detailed design phase.

4.2 Loss of Safeguard Building HVAC System Safety Case

4.2.1 Summary of EDF and AREVA's Safety Case

118 Faults in this category result in the total or partial loss of the normal safeguard building HVAC systems. Such faults can potentially produce multiple consequences. For example, loss of the HVAC system can result in the loss of cooling to C&I systems and essential electrical systems with consequential loss of the frontline systems that these systems support.

119 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 either partial or complete loss of the safeguard building main HVAC systems. For those cases which they consider to be limiting, they have performed detailed analyses.

120 In the case of partial loss of a safeguard building main HVAC system, EDF and AREVA claim that these studies demonstrate that adequate redundancy is provided on the UK EPR™ even after taking account of the most onerous single failure, the worst plant maintenance state and the assumed consequential loss of off-site power, such that at least one of the safeguard divisions remains available and that this is sufficient to provide adequate cooling of the reactor even assuming seal LOCAs in all four RCPs.

121 In the case of common mode failure within a safeguard building main HVAC system, EDF and AREVA claim that the new designs for safeguard building main and diverse HVAC systems provides sufficient diversity within the design that only two trains of HVAC system would be lost due to a common mode failure and that this possibility is bounded by the single failure analysis already presented.

122 On the basis of the analysis presented, EDF and AREVA have concluded that adequate protection against loss of safeguard building main HVAC system faults is provided for all the range of faults considered.

4.2.2 Assessment

123 EDF and AREVA have identified the following faults within this category that they consider to be the limiting single failures (Refs 13 and 16):

- Loss of a single ventilation train in the safeguard building main HVAC system.
- Loss of a single chilled water train in the safeguard building main HVAC system.

124 In addition, EDF and AREVA identify the following faults within this category that they consider to be the limiting common mode failures (Refs 14 and 16):

- Total loss of two ventilation trains in the safeguard building main HVAC system in divisions (1 & 4 or 2 & 3) with external air temperature less than 25°C.
- Total loss of two chilled water trains in the safeguard building main HVAC system in divisions (1 & 4 or 2 & 3) with external air temperature less than 25°C.
- Total loss of two chilled water trains in the safeguard building main HVAC system in divisions (1 & 4 or 2 & 3) with external air temperature greater than 25°C.

125 In the sections below, I have separately presented my assessment of partial failure of a safeguard building main HVAC system (Section 4.2.2.1) from my assessment of total failure of a safeguard building main HVAC system (Section 4.2.2.2).

4.2.2.1 Partial Loss of Safeguard Building Main HVAC System

System Description of the Safeguard Building Main and Diverse HVAC Systems

126 Before reviewing the fault sequence analysis it is worth reviewing the system designs for the safeguard building main and diverse HVAC systems.

127 The role of the safeguard building main HVAC system is to maintain acceptable ambient temperature conditions and air renewal conditions for staff and equipment in the uncontrolled area of the four safeguard buildings, particularly the electrical, electronic and mechanical rooms. The safeguard building main HVAC system is a four 100% train system that is supplied from four independent electrical trains. Each train of the system is located in a different safeguard building and consists of a ventilation train cooled by a chilled water train. The chilled water trains in Divisions 1 and 4 are air cooled and are also used to provide diverse cooling to the LHSI pump motors and bearings in their division should the associated CCWS trains fail. The chilled water trains in Divisions 2 and 3 are cooled by the common header of the associated CCWS trains. The LHSI pump motors in these Divisions are only cooled by their associated CCWS train. Each of the four chilled water trains also provides cooling to the other HVAC systems in the safeguard buildings including if so aligned 50% cooling to MCR HVAC system.

128 In Chapter 9.4 of the PCSR (Ref. 22), EDF and AREVA confirm that the system is required to meet the single failure criteria, have electrical supplies that are backed-up by EDGs, and be seismically qualified. Divisions 1 and 4 are also backed-up by the UDGs. EDF and AREVA claim that the design has considered internal and external hazards.

129 In developing a response to GDA issue **GI-UKEPR-FS-05**, EDF and AREVA have upgraded the classification of the ventilation trains and the chilled water trains of the safeguard building main HVAC system to Class 1 under CMF#41 (Ref. 8) as part of a fundamental redesign of the safeguard building HVAC systems for the UK EPR™. The conceptual design for this modification (Ref. 19) is discussed further below.

130 Following the loss of any one train of the safeguard building main HVAC system, cooling is automatically switched to one train of the safeguard building diverse HVAC system.

131 The role of the safeguard building diverse HVAC system is to provide a backup standby system to the safeguard building main HVAC system. The safeguard building diverse HVAC system is a two 100% train system that is supplied from two independent electrical trains in Divisions 1 and 4. One train of the safeguard building diverse HVAC system is also used to provide cooling when maintenance is performed on one train of the safeguard building main HVAC system. Maintenance will only be allowed when the external air temperature is below a specified value currently assumed to be 25°C although this will need to be confirmed during the site specific detailed design phase. One train of the system is located in safeguard building 1 and supplies either Divisions 1 or 2 as required. The other train of the system is located in safeguard building 4 and supplies either Divisions 3 or 4 as required. Each train of the system consists of a ventilation train cooled by a chilled water train. The chilled water trains are air cooled and will be located in plant rooms at roof level in safeguard buildings 1 and 4. EDF and AREVA confirm that the system will have diverse electrical supplies.

132 In developing a response to GDA issue **GI-UKEPR-FS-05**, EDF and AREVA have significantly redesigned the safeguard building diverse HVAC system under CMF#77 (Ref. 8) as part of a fundamental redesign of the safeguard building HVAC systems. The conceptual design for this modification (Ref. 19) is also discussed further below.

Fault Sequence Analysis

133 EDF and AREVA have treated the two single failure faults listed above as design basis faults meeting the requirements of FA.4 and FA.5 although they have not formally allocated them as PCC events within the PCSR but as "specific studies". I therefore consider that Assessment Finding **AF-UKEPR-FS-90**, which requires a future licensee to include these events within the design basis analysis of a site specific PCSR, to be equally applicable to the partial loss of safeguard building main HVAC faults as well. However, as with the loss of cooling chain faults, I recognise that the deterministic assessment performed does assume the most onerous single failure and the worst plant maintenance condition together with consequential LOOP following reactor trip so my judgement is that in practice the requirements of SAPs FA.6, EDR.2 and EDR.4 are being met although the radiological assessment still has to be presented. In addition to the deterministic assessment and as part of the site specific detailed design phase, it will also be necessary to model loss of the safeguard building main HVAC system faults within the PSA to confirm the balance of risk is ALARP when judged against SAPs T.8 and T.9. I therefore consider that Assessment Finding **AF-UKEPR-FS-91**, which requires a future licensee to perform such an assessment, is equally applicable to these faults.

134 EDF and AREVA state (Refs 14 and 16) that the initiating frequency for loss of either one ventilation train or one chilled water train of the safeguard building main HVAC system is 1×10^{-2} per year. EDF and AREVA therefore acknowledge that these events are both frequent faults. For this reason, they have performed a diversity analysis for common mode failure of frontline systems on demand in coincidence with these initiating events (Ref. 21) which I have assessed in my close-out report (Ref. 25) for Action 8 of GDA Issue **GI-UKEPR-FS-02** on functional diversity for frequent faults.

135 EDF and AREVA have performed a deterministic assessment (Refs 13 and 16) to establish the consequences of these single failure faults when coupled with the assumption of the most onerous single failure, the worst plant maintenance condition, and a consequential LOOP. As with the loss of cooling chain fault assessed in Section 4.1.2.1 above, in my judgement, the approach is systematic and comprehensive. For each initiating fault, a series of tables are completed in which each single failure and plant maintenance are analysed together with the assumption of LOOP.

136 While the same plant maintenance states are considered an additional single failure is added to the list of single failures considered:

- Failure of automatic switchover to a safeguard building diverse HVAC train.

137 Some general characteristics can be noted. The combination of the safeguard building main and diverse HVAC systems provides for six redundant HVAC trains when compared with the four redundant CCWS / ESWS trains and four redundant electrical divisions. Hence, the single failure safeguard building HVAC fault is generally less onerous than single failures on these other systems since it takes a combination of the initiating event with either a plant maintenance state or a single failure to create the reactor trip that is needed to cause consequential LOOP. This means that the loss of only one EDG needs to be considered in coincidence with LOOP and so generally more safeguard divisions remain available to cope with these faults than for the partial loss of cooling chain faults considered in Section 4.1.2.1 and partial loss of electrical systems considered in Section 4.6.2.1. The design basis faults identified below which assume that only one safeguard division remains available to protect against the fault are therefore very conservative for the partial loss of safeguard building main HVAC system faults.

138 Depending upon which single failures and plant maintenance states are considered it is still possible for a seal LOCA to occur on the four RCPs. Depending upon which single failures and plant maintenance states are considered it is still possible for both EBS trains to be lost for intact circuit sequences.

139 In developing the safety case EDF and AREVA have proactively identified the need for a number of design changes to ensure compliance with the design basis analysis rules. These design changes are generally associated with an upgrading in the safety classification of the C&I systems that are claimed to actuate engineered safeguards such as the switchover to a safeguard building diverse HVAC train. However they have also identified the need to provide additional functionality to improve protection against these faults including provision of two new chilled water trains for the safeguard building diverse HVAC system as explained in a conceptual design note (Ref. 19). The design changes identified are discussed in the following paragraphs. Progress with these modifications will be monitored by ONR during the site specific detailed design phase through the generic cross cutting Assessment Finding **AF-UKEPR-CC-01** (Ref. 27) which requires a future licensee to implement any design changes identified during GDA.

140 CMF#41 (Ref. 8) covers the following design changes:

- The ventilation and chilled water trains of the safeguard building main HVAC system will be upgraded to Class 1 which will also include the use of Class 1 C&I.
- The ventilation trains of the safeguard building diverse HVAC system will be upgraded to Class 1.
- The new chilled water trains of the safeguard building diverse HVAC system will be provided at Class 2 and will be air cooled.
- Maintenance will only be allowed on the safeguard building HVAC systems when the outside temperature is below 25°C.
- Automatic switchover from a safeguard building main HVAC ventilation train to a safeguard building diverse HVAC ventilation train will be upgraded to Class 1.
- Automatic switchover from a safeguard building main HVAC chilled water train to a safeguard building diverse HVAC chilled water train will be upgraded to Class 2.
- The safeguard building diverse HVAC system will be automatically supplied by the EDGs at Class 1 and powered from the 400 V switchgear instead of the 690 V switchgear used by the safeguard building main HVAC system.
- The mechanical design of trains 1 and 4 of the safeguard building main HVAC system will be diverse from the mechanical design of trains 2 and 3.
- The mechanical design of the safeguard building main HVAC system will be diverse from that of the safeguard building diverse HVAC system.
- The control system design of the safeguard building main HVAC system will be diverse from that of the safeguard building diverse HVAC system.
- Loss of both the PS and SAS shall be considered within the design. One possible solution would be for the C&I on the safeguard building diverse HVAC system to be implemented using the UNICORN technology that is being applied to the NCSS if it can be upgraded to Class 1.

141 In addition, CMF#78 (Ref. 8), discussed in Section 4.6.2.2 below, and covering changes to the essential electrical system, is also relevant as it covers provision of diverse electrical supplies to the safeguard building diverse HVAC system. Although this design

change is welcomed, my preference would have been for the power supplies of the safeguard building diverse HVAC system to have been supplied from the battery backed uninterruptible power supplies (UPS) since this would ensure that the electrical supplies for the safeguard building diverse HVAC system would be the same as those used to supply the C&I systems that the HVAC system cools. This safety principle was applied to the design of Sizewell B and in my judgement represents good practice in the UK. It ensures that whenever a consumer is being supplied with electrical power and so needs to dissipate heat, then the HVAC system that is needed to cool it will also have the same electrical supplies available. Technically, it is minimizing the number of minimum cutsets and simplifying the design so increasing the overall reliability.

142 Instead EDF and AREVA are following an alternate strategy which aims to demonstrate that the thermal inertia of the safeguard building is sufficient to avoid the C&I and electrical systems over heating before the batteries are drained of power. The analysis justifying this claim is discussed further in Section 4.6.2.2 below.

143 Although the modifications under CMF#41 are already covered by generic Assessment Finding **AF-UKEPR-CC-01** (Ref. 27), it is recognised that the design is only at the conceptual stage at the moment and needs to be developed further during the site specific detailed design phase. I have therefore raised Assessment Finding **AF-UKEPR-FS-101** for a future licensee to further develop CMF#41 into a more detailed design specification. Given the potential implications to plant layout of these design changes, it is considered essential that this analysis and design work is substantially completed early in the site specific detailed design phase and prior to the pouring of Nuclear Island safety-related concrete.

144 It should be noted that the design modifications proposed under CMF#39 and CMF#75 (Ref. 8) discussed in Section 4.1.2.1 above are equally applicable for the partial loss of the safeguard building main HVAC system.

145 As a result of the fault sequence analysis, which assumes the above modifications are in place, EDF and AREVA conclude (Refs 13 and 16) that for the reactor the same design basis faults bound these fault sequences as the partial loss of cooling chain faults discussed in Section 6.1.2.1 above. That is the following faults:

- Two tripped RCPs with loss of three safeguard building divisions.
- Four RCP seal LOCAs with loss of three safeguard building divisions.

146 I agree with this conclusion and consider it to be conservative for faults resulting in the partial loss of the safeguard building main HVAC system providing the proposed modifications discussed above and covered by Assessment Findings **AF-UKEPR-CC-01** and **AF-UKEPR-FS-101** are fully implemented. I therefore judge that the functional analysis performed by EDF and AREVA to identify these sequences meets the requirements of SAPs FA.6, EDR.2 and EDR.4.

Transient Analysis

147 The limiting design basis events defined above are the same as those covering the partial loss of cooling chain faults discussed in Section 4.1.2.1. Hence the transient analysis studies (Ref. 15) that I have already assessed in Section 4.1.2.1 are equally applicable for partial loss of safeguard building main HVAC faults. Hence, in my judgement the requirements of SAP FA.7 are met for these faults as well.

4.2.2.2 Total Loss of a Safeguard Building Main HVAC System

Fault Sequence Analysis

148 The PCC analysis rules of EDF and AREVA do not apply to faults caused by a common mode failure. Nevertheless, EDF and AREVA acknowledge that such events occur with a frequency of about 10^{-5} per year (Ref. 14) and so have performed a design basis analysis for this fault consistent with UK practice in which additional failures are considered if the resultant sequence frequency is still greater than 10^{-7} per year (Ref. 7).

149 In practice, this has required EDF and AREVA to consider an additional plant maintenance state when the external air temperature is below 25°C but not an additional single failure or consequential LOOP. EDF and AREVA do not consider an additional plant maintenance state when the external air temperature is above 25°C on the grounds that the conditional probability for such a condition is approximately 1×10^{-2} per demand. In my judgement, this approach meets the requirements of SAPs FA.4 and FA.5.

150 In developing the safety case EDF and AREVA have proactively identified the need for a number of design changes. These design changes are covered by CMF#41 (discussed in Section 4.2.2.1 above).

151 As a result of the fault sequence analysis, which assumes the above modifications are in place, EDF and AREVA conclude (Ref. 16) that there is no need for any new design basis faults as the fault sequences that have been identified are already bounded by the same transient studies performed for single failure faults assessed in Section 4.2.2.1 above.

152 The position of EDF and AREVA is best understood with reference to their probabilistic assessment (Ref. 14) used to determine the initiating frequencies for these events. This presents an assessment performed using very simple fault and event tree models of the safeguard building main and diverse HVAC systems.

153 The analysis makes a number of simplifying assumptions. It does not model the essential electrical support system although it does represent the C&I support systems. It discounts the probability for failure to start for those systems that are already in operation and it assumes that mechanical diversity has been achieved between trains 1 and 4 and trains 2 and 3 of the main HVAC system as well as between the trains of the main and diverse HVAC systems. A common mode failure beta factor[1] of 0.05 is applied to redundant but otherwise identical trains. It also assumes that the ventilation trains will provide sufficient cooling to the safeguard buildings even if the chilled water trains fail providing the external air temperature is below 25°C. The conditional probability of the external air temperature being higher is 2×10^{-2} per demand and the conditional probability for a plant maintenance state is assumed to be 2×10^{-2} per demand. Only automatic actions are claimed.

154 The results predict that the failure of one train is a frequent event at 1.4×10^{-2} per year and the failure of two trains is 1.5×10^{-5} per year consistent with the discussion above. The results predict very low probabilities for failure of more than two or three trains and these events tend to be dominated by failure of the C&I systems. As already noted,

[1] The random failure for the probability of failure-on-demand on n redundant divisions where each division has a failure probability of p is given by the formula $P = p^n$ assuming each division is capable of delivering the full function (n x 100%). However, this doesn't take into account common cause failures. These can be modelled many ways but one method is to derive what is known as a beta factor (β) from empirical dependant failure analysis of the system. The formula for the probability of failure on demand then becomes $P = p^n + \beta p$.

common mode failure of the 690 V AC electrical support system that provides electrical supplies to all four trains of the safeguard building main HVAC system is not modelled. However, I do assess the safety case with regard to such a failure in Section 4.6.2.2 below.

155 I have not performed an assessment of the models or the data and so will not comment on the predicted frequencies. Nevertheless, the assumptions made in the analysis have implications for the safety case and as a consequence the engineering design. EDF and AREVA have recognised this in the conceptual design note (Ref. 19) for the design of the safeguard building main and diverse HVAC systems. As well as proposing that each train of the safeguard building main HVAC system will be physically segregated into different safeguard buildings, the intention is that the mechanical design for trains 1 and 4 will be diverse from trains 2 and 3 as well as from that of the diverse HVAC system. A future licensee will need to demonstrate this has been achieved in practice as part of the response to **AF-UKEPR-FS-101**. It will also be necessary to substantiate the claim that the ventilation train can provide adequate cooling of the safeguard building following failure of its associated chilled water train. Finally, three C&I platforms including the PS and the SAS and possibly a UNICORN based design are being considered to meet the reliability targets.

156 In my judgement, providing these claims can be demonstrated within the design substantiation document for these systems then the three sequences listed above, in which common mode failure of two trains together with a plant maintenance state (or high external air temperature) is taken as the design basis are reasonable and will meet the requirements of SAPs FA.6 and EDR.2 to EDR.4.

Transient Analysis

157 The limiting design basis events defined above are bounded by those covering the partial loss of cooling chain faults discussed in Section 4.1.2.1. Hence the transient analysis studies (Ref. 15) that I have already assessed in Section 4.1.2.1 are equally applicable for common mode failure of safeguard building main HVAC faults. Hence, in my judgement the requirements of SAP FA.7 are met for these faults as well subject to satisfactory resolution of **AF-UKEPR-FS-101**.

4.2.3 Findings

158 Following my assessment of the EDF and AREVA submissions, I am content for GDA issue **GI-UKEPR-FS-05** to be closed with regard to the safeguard building main and diverse HVAC systems. Assessment Finding **AF-UKEPR-FS-101** has been raised for a future licensee to complete the conceptual designs for the safeguard building main and diverse HVAC systems. Given the preliminary nature of the design and the importance of these systems this Assessment Finding needs to be closed out prior to the pouring of Nuclear Island safety-related concrete.

4.3 Loss of other HVAC Systems Safety Case

4.3.1 Summary of EDF and AREVA's Safety Case

159 Faults in this category result in the total or partial loss of any HVAC system other than the safeguard building main HVAC system considered in the Section 4.2. Such faults can

potentially produce multiple consequences. For example, loss of an HVAC system can result in the loss of cooling to C&I systems with consequential loss of any associated frontline systems that they support.

160 The basis of the safety case of EDF and AREVA 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 the complete loss of one of these other HVAC systems. For those cases which they consider to be limiting, they have performed detailed analyses.

161 With the exception of the MCR HVAC system and the Circulating Water (CW) pump house HVAC system, EDF and AREVA conclude that failure of these systems will only result in reactor transients that are already covered by pre-existing design basis faults. In the case of the MCR HVAC system and the pump house HVAC system, EDF and AREVA are proposing a series of design changes to provide additional protection against such faults.

162 EDF and AREVA conclude that on the basis of the functional analysis presented adequate protection is provided against these faults subject to further work during the site specific detailed design phase.

4.3.2 Assessment

163 In their assessment of the loss of other HVAC system faults, EDF and AREVA have adopted a screening approach in which a common mode failure is assumed to occur on each of these other HVAC systems in turn to determine whether such a fault will result in either a reactor or a spent fuel pool transient and if it does whether these events are bounded by pre-existing PCC analysis. No account is taken of other faults occurring at the same time. For those cases not covered by pre-existing PCC analysis, EDF and AREVA also aimed to establish whether adequate mitigation is in place or identify further actions to be taken forward into the site specific detail design phase.

164 In addition to the safeguard building main and diverse HVAC systems assessed in Sections 4.2.2.1 and 4.2.2.2 above, there are sixteen HVAC systems on the UK EPR™ (Ref. 20). Of these systems, I have chosen to sample the functional analysis that EDF and AREVA have performed of the following ventilation systems (and their associated chilled water systems) on the grounds that together with the safeguard building main and diverse HVAC systems considered in Section 4.2, these HVAC systems are the ones that are equivalent to the HVAC systems on Sizewell B that attract a *safety category 1* designation, which is equivalent to Class 1 on the UK EPR™:

- MCR air conditioning system
- Remote shutdown station air conditioning system
- Fuel building ventilation system
- Diesel room ventilation system
- Reactor building ventilation system
- Pumping station ventilation system
- Safeguard auxiliary buildings ventilation system (controlled area)

165 EDF and AREVA have yet to assign safety classifications to these systems. This will be performed during the site specific detailed design phase in response to the generic Assessment Finding **AF-UKEPR-CC-05** and will depend on the safety classification of

safety systems that these HVAC systems support. Each of these systems is reviewed in turn in the following paragraphs.

166 The purpose of the MCR air conditioning system is to maintain acceptable temperatures and humidity levels in the MCR during normal operation and accident conditions for the proper operation of personnel and equipment. It also provides habitability protection for events resulting in radiological contamination. It consists of four physically independent air conditioning trains each with 50% capacity that in the current design are cooled by the chilled water trains of the safeguard building main HVAC system. EDF and AREVA accept that there are no elements of diversity within the current design (Ref. 16) and that common mode failure of the MCR air conditioning system will result in the temperature rising above 32°C in 40 minutes (Ref. 20). If the situation continues it will result in the overheating of critical electrical equipment located in the MCR and associated computer rooms.

167 CMF#77 (Ref. 8) therefore proposes to perform an ALARP assessment to identify the optimum design changes needed to improve the protection provided for such faults. These include the following basic proposals (Ref. 16):

- Upgrade of the MCR air conditioning system to Class 1 including upgrading the automatic switchover from a duty to a standby train to Class 1.
- The introduction of diverse mechanical designs between trains 1 and 4 and trains 2 and 3.
- Increasing the capacity of the trains to provide four 100% trains.

168 Additional options include:

- Provision of diverse C&I protection system.
- Introduction of diverse cooling/chilled water trains.
- Provision of diverse electrical supplies from the 400 V switchboards.
- Provision of a completely new diverse MCR air conditioning system.

169 Although this design change proposal is covered by the generic Assessment Finding **AF-UKEPR-CC-05** clearly the proposed design changes are at very preliminary stage of development. EDF and AREVA state that they have not yet considered the implications of these design changes on plant layout which will also be affected by the choice of location of the NCSS (Ref. 16). In my judgement, given the potential implications to plant layout of these changes, it is essential that this analysis and design work is substantially completed early in the site specific detailed design phase. I have therefore raised Assessment Finding **AF-UKEPR-FS-102** for a future licensee to further develop these design change proposals prior to the pouring of Nuclear Island safety-related concrete.

170 The purpose of the remote shutdown station is to provide a diverse location for the operator to bring the plant to a safe shutdown state following events that lead to the MCR becoming unavailable. Currently the safety classification of the remote shutdown station HVAC system is Class 3 which contrasts with the situation at Sizewell B. EDF and AREVA acknowledge (Ref. 20) that a justification of the current design or identification of improvements will be required as part of CMF#77 discussed in the previous paragraphs. I consider that this requirement is also covered by Assessment Finding **AF-UKEPR-FS-102**.

171 The purpose of the fuel building HVAC system is to automatically isolate either the spent fuel pool hall or the reactor building following either a fuel handling accident or the loss of

the main FPCS and to maintain temperatures in the equipment rooms including the boron rooms to ensure the correct operation of the FPCS pumps, the EBS pumps, the CVCS pumps, and the reactor borated water make-up system. EDF and AREVA argue that failure of these systems would not result in a situation that is not already covered by pre-existing design basis analysis but recognise there is need to demonstrate the possibility of such a fault occurring has been reduced to ALARP. In particular, the design of the operational chilled water system that provides the heat sink function for part of the fuel building ventilation system needs to be reviewed. I agree with this conclusion and have raised Assessment Finding **AF-UKEPR-FS-103** for a future licensee to perform a further review of the fuel building HVAC system during the site specific detailed design phase to ensure that the design is ALARP.

172 The purpose of the diesel room ventilation system (Ref. 20) is to remove the heat radiated from the diesel generators and the heat dissipated by the electrical equipment since the diesels themselves are cooled by systems independent of the HVAC. EDF and AREVA conclude that as the diesel room ventilation system does not operate during normal operation it cannot be the initiator for a design basis fault. I agree with this conclusion but note that the same ventilation system cools both the EDG room and the UDG room. Given that LOOP is a very frequent initiating event the intention is that these diesels provide diverse protection against the fault. In my report covering the close out of Action 8 of GDA issue **GI-UKEPR-FS-02** (Ref. 25) I have raised Assessment Finding **AF-UKEPR-FS-45** requesting a future licensee to consider a common mode failure in each of the essential support systems for the list of frequent faults. Clearly, this review will need to consider the consequences of common mode failure of the diesel room ventilation system.

173 There are two HVAC systems in the reactor building (Ref. 20). The first system is the containment cooling ventilation system which provides continuous cooling of the containment including the reactor vessel pit during normal operation. The role of the system includes cooling the control rod drive mechanisms and the ex-core neutron flux detectors and associated instrumentation. EDF and AREVA acknowledge that further work is required to fully understand the implications of loss of HVAC on the control rod mechanism and the ex-core instrumentation but argue that there is likely to be a considerable grace period for the operator to intervene before a reactor transient could occur. I have raised Assessment Finding **AF-UKEPR-FS-104** for a future licensee to establish what the consequences are for these systems following the loss of the containing cooling ventilation system.

174 The second system is the containment sweep ventilation system which is provided for purging the containment to prevent radiological releases. This system does not operate during normal operation and so cannot initiate a design basis fault.

175 The purpose of the CW pump house HVAC system (Ref. 20) is to maintain ambient conditions within the pump house including the ESWS tunnels and fire pump room to ensure the satisfactory operation of the safety systems located in the building including the ESWS, CWFS and the UCWS. EDF and AREVA argue (Ref. 20) that loss of the CW pump house HVAC system is bounded by the total loss of cooling chain fault on the grounds that thermal analyses demonstrate that the UCWS does not require cooling by the system. However, these thermal analyses have not been shared with ONR. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-105** for a future licensee to provide the substantiation evidence to justify the time periods that are being claimed.

176 EDF and AREVA acknowledge that it is important that the reliability of the CW pump house HVAC system should not dominate the initiating frequency for total loss of cooling

chain fault and have therefore proactively identified the need for a number of design changes that are covered under CMF#80.

177 CMF#80 (Ref. 8) proposes the following design changes:

- Upgrading to Class 1 the temperature sensors located in the ESWS shaft to provide an alarm to the operator on the loss of CW pump house HVAC system providing the grace time can be demonstrated to be long enough to justify manual action for performing the recovery operations.
- Upgrading to Class 1 of the C&I associated with the start-up and control of the CW pump house HVAC if the grace time is not sufficient to justify manual recovery.

178 An additional option includes:

- The introduction of manufacturing diversity for sensitive mechanical components in two of the four trains of the CW pump house HVAC system to ensure that the reliability of the HVAC system does not dominate the initiating frequency for total loss of cooling chain faults.

179 Although this design change proposal is covered by the generic Assessment Finding **AF-UKEPR-CC-05** clearly the proposed design changes are at very preliminary stage of development. In my judgement, given the potential implications to plant layout of these changes, it is essential that this analysis and design work is substantially completed early in the site specific detailed design phase. I have therefore raised Assessment Finding **AF-UKEPR-FS-106** for a future licensee to further develop these design change proposals prior to the pouring of Nuclear Island safety-related concrete.

180 The purpose of the safeguard building controlled area HVAC system (Ref. 20) is to maintain the dynamic containment of the controlled areas of the safeguard buildings and the spent fuel pool hall and to provide cooling of the important safeguard equipment located within these areas. The latter includes rooms that contain components of the following systems; the CCWS and EFWS valve room, the FPCS room (containing components for the 3rd train of the FPCS), the CHRS room, the safety injection system pump room, safety injection system heat exchanger room, the safety injection system valve room, and the sump valve room.

181 EDF and AREVA argue that with the exception of the CCWS and the LHSI pumps (when the latter are performing in RHR mode during shutdown operations), these safety systems do not operate during normal operation and so cannot initiate a design basis event. I have already assessed the total loss of CCWS fault in Section 4.1.2.2 above. In the case of the LHSI pumps, EDF and AREVA claim (Ref. 20) that thermal analysis performed for FA3 demonstrates that the LHSI pumps would continue to operate for up to fifteen days following loss of the HVAC cooling with an external ambient temperature not greater than 36°C when assessed against a safety limit of 60°C and for longer with just the loss of the chilled water train and an external temperature of 25°C. EDF and AREVA therefore conclude that following the total loss of the safeguard building controlled area HVAC system the LHSI pumps in RHR mode would continue to operate for a sufficient period.

182 In their response to TQ-EPR-1621 (Ref. 9), EDF and AREVA make similar claims about the capability of the EFWS pumps to continue to operate for fifteen days following failure of the chilled water trains of the safeguard building main HVAC system while failure of the ventilation trains will not result in their failure for seven days. However, these thermal analyses have not been shared with ONR. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-107** for a future licensee to provide the substantiation evidence to justify the time periods that are being claimed.

183 EDF and AREVA note (Ref. 20) that the operational chilled water system supports a number of ventilation systems including the containment cooling ventilation system, the nuclear auxiliary building ventilation system, the fuel building ventilation system, the ventilation systems for the main steam system, the feedwater control system, the steam generator blowdown system valve compartment. Although they claim its failure cannot initiate a new design basis event they propose to perform further studies during the site specific detailed design phase to ensure that the current design is ALARP. I consider that Assessment Finding **AF-UKEPR-FS-103** that was raised above in the context of the fuel building also covers this work.

184 In summary, as a result of this work, EDF and AREVA have identified the following faults where further work will be required (Ref. 16) to provide a satisfactory design basis safety case:

- Total loss of main control room ventilation system.
- Total loss of CW pumping station ventilation system.

185 Given the above discussion, I agree with this conclusion. In my judgement, the functional analysis presented by EDF and AREVA meets the requirements of SAPs FA.4 to FA.6 and EDR.2 to EDR.4. I also judge that sufficient progress has been made to justify closure of GDA issue **GI-UKEPR-FS-05** with regard to these other HVAC systems subject to completion of the modifications proposed under CMF#77 and CMF#80 during the site specific detailed design phase.

4.3.3 Findings

186 Following my assessment of the EDF and AREVA submissions, I am content for GDA issue **GI-UKEPR-FS-05** to be closed with respect to these other HVAC systems. Assessment Findings **AF-UKEPR-FS-102** to **AF-UKEPR-FS-107** have been raised.

4.4 Loss of Instrument Air Systems Safety Case

4.4.1 Summary of EDF and AREVA's Safety Case

187 Faults in this category result in the total or partial loss of the instrumentation air systems.

188 The basis of the safety case of EDF and AREVA is that they have performed a functional analysis of the consequences of total loss of the instrument air systems and concluded that failure of these systems will only result in reactor transients that are already covered by other design basis faults.

189 EDF and AREVA conclude that on the basis of the functional analysis presented adequate protection is provided against these faults.

4.4.2 Assessment

190 In their assessment of the loss of instrument air system faults, EDF and AREVA have adopted the same screening approach applied to the loss of HVAC systems in which a common mode failure is assumed to occur on each of the instrument air systems in turn to determine whether it will result in either a reactor or a spent fuel pool transient and if it does whether these events are bounded by pre-existing PCC analysis. No account is

taken of other faults occurring at the same time. EDF and AREVA also aimed to establish whether adequate mitigation is in place or identify further actions to be taken.

191 There are three instrument air systems on the UK EPR™ (Refs 13, 16 and 22). These are the following:

- Compressed air production system.
- Working compressed air distribution system.
- Control compressed air distribution system.

192 The compressed air production system supplies clean air to the two other systems. The working compressed air distribution system supplies air to pneumatic tools and equipment. The control compressed air distribution system supplies air to pneumatic valves and pneumatic control valves some of which are within the nuclear island. EDF and AREVA claim that only the control compressed air distribution system has a safety significant role.

193 If there is a loss of air pressure in the compressed air distribution network automatic valves isolate the working compressed air distribution system and the conventional island sections of the control compressed air distribution system to prioritise supply to the nuclear island sections. As a last reserve, local buffer tanks on the control compressed air distribution system enable the safety pneumatic valves to operate for two movements per supplied valve taking account of air leakage during 24 hours. EDF and AREVA claim that these pneumatic valves move to a fail-safe position following loss of air although it is unclear to me how this can be achieve for all the actuators listed below.

194 The systems that the control compressed air system on the UK EPR™ (Refs 13, and 16) provides compressed air to include the following:

- MFWS valves (for which buffer tanks are not provided).
- Motor-driven feedwater pump system.
- Circulating water system.
- Start-up / stand-by feedwater system.
- Main steam by-pass system.
- Pneumatic valves on the CCWS.
- Nuclear vent and drainage system.

195 EDF and AREVA conclude that of the three instrument air systems on the UK EPR™ only the loss of the control compressed air system will result in reactor transients and that these are bounded by two pre-existing design basis faults. These are the PCC-2 loss of main feedwater fault assessed in the GDA Step 4 Fault Studies report (Ref. 2) and the break in a single CCWS common header fault discussed in Section 4.1.2.1 above. EDF and AREVA therefore conclude that no new design basis accidents need to be considered. Despite my comments about the claim on fail safe positions for the actuators, given the list of services that the instrument air systems support, I agree with the overall conclusion that no new design basis events need to be considered. Under the generic Assessment Finding **AF-UKEPR-CC-05**, a future licensee will need to determine the safety classification of the instrument air systems based upon the safety systems they support.

196 I note that of the four compressed air systems on Sizewell B, only the clean air system is a *safety category 1* system. It is used to power the SG Power Operated Relief Valves

(PORVs) and to open the valves on the steam turbine driven auxiliary feedwater system. These are important safety systems on Sizewell B.

4.4.3 Findings

197 Following my assessment of the EDF and AREVA submissions, I am satisfied that the loss of instrument air systems cannot result in a new design basis fault that is not already covered by the existing PCC analysis. For this reason, I am content that GDA issue **GI-UKEPR-FS-05** can be closed with regard to the instrument air systems. I have no additional Assessment Findings.

4.5 Loss of Nitrogen Gas Distribution Systems Safety Case

4.5.1 Summary of EDF and AREVA's Safety Case

198 Faults in this category result in the total or partial loss of the nitrogen gas distribution systems.

199 The basis of the EDF and AREVA safety case is that they have performed a functional analysis of the consequences of total loss of the nitrogen gas distribution system and concluded that failure of the system could not result in a fault transient occurring on the reactor.

200 EDF and AREVA conclude that on the basis of the functional analysis presented adequate protection is provided against these faults.

4.5.2 Assessment

201 In their assessment of the loss of nitrogen gas distribution system faults, EDF and AREVA have adopted the same screening approach applied to the loss of HVAC systems and the loss of instrument air systems, in which a common mode failure is assumed to occur in the nitrogen gas distribution system to determine whether it will result in either a reactor or a spent fuel pool transient and if it does whether this event is bounded by pre-existing PCC analysis.

202 The nitrogen gas distribution system on the UK EPR™ (Refs 13 and 16) serves the following functions:

- Flushing and/or filling of various tanks and systems including the primary circuit and the accumulators during normal and/or shutdown operations.
- Actuation of the SSSS following RCP tripping due to loss of cooling of the RCP thermal barriers.
- Operation of the Aeroball measuring system.

203 EDF and AREVA conclude that total loss of the nitrogen gas distribution system will not result in any transient on the reactor or the spent fuel pool and that therefore no new design basis accidents need to be considered. Given the list of services that the nitrogen gas distribution system supports, I agree with this conclusion. While failure of the nitrogen gas distribution system could potentially result in the failure of the SSSS on demand (and only then if buffer tanks are not provided local to the SSSS), the SSSS does not operate during normal operation and so failure of the distribution system cannot cause

a reactor transient by itself. It must also be recognised that the SSSS currently has a low safety classification. In my judgement, use of the nitrogen gas distribution system as a source of motive power that is diverse from AC electrical power is a good idea since one of the most important fault sequences that the SSSS provides some mitigation against is the SBO sequence. Under the generic Assessment Finding **AF-UKEPR-CC-05**, a future licensee will need to determine the safety classification of the nitrogen gas distribution system based upon the safety systems its supports.

204 I note that the nitrogen gas distribution system on Sizewell B is a *safety category 1* system. It is used as a diverse means to power the SG PORVs and to open the valves on the steam turbine driven auxiliary feedwater system should the clean air supply fail. These are important safety systems on Sizewell B.

4.5.3 Findings

205 Following my assessment of the EDF and AREVA submissions, I am satisfied that loss of the nitrogen gas distribution system cannot result in a fault transient occurring on the reactor. For this reason, I am content that GDA issue **GI-UKEPR-FS-05** can be closed with regard to the nitrogen gas distribution system. I have no additional Assessment Findings.

4.6 Loss of Essential Electrical Systems Safety Case

4.6.1 Summary of EDF and AREVA's Safety Case

206 Faults in this category result in the total or partial loss of normal on-site electrical 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.

207 The basis of the safety case of EDF and AREVA 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 either partial or complete loss of the essential electrical systems. For those cases which they consider to be limiting, they have performed detailed analyses.

208 In the case of partial loss of an essential electrical system, EDF and AREVA claim that these studies demonstrate that adequate redundancy is provided on the UK EPR™ even after taking account of the most onerous single failure, the worst plant maintenance state and the assumed consequential loss of off-site power, such that at least one of the safeguard divisions remains available and that this is sufficient to provide adequate cooling of the reactor even assuming seal LOCAs in all four RCPs.

209 In the case of common mode failure of a common voltage level within the essential electrical systems, EDF and AREVA claim that the proposed design changes to the allocation of electrical loads to different switchboards will ensure that diverse electrical supplies are provided for each required safety function such that a controlled state can be reached.

210 EDF and AREVA conclude that on the basis of the functional analysis presented adequate protection is provided against these faults subject to further work during the site specific detailed design phase.

4.6.2 Assessment

211 EDF and AREVA have identified the following faults within this category that they consider to be the limiting single failures (Refs 13 and 16):

- Loss of supplies from one 10 kV AC (LHi) switchboard.
- Loss of supplies from one 690 V AC (LJi) switchboard.
- Loss of supplies from one 400 V AC (LVi) UPS switchboard.
- Loss of supplies from one emergency supplied 400 V AC (LLi) switchboard.
- Loss of supplies from one regulated 230/400 V AC (LOi) switchboard.
- Loss of supplies from one 220 V Direct Current (DC) (LAi) switchboard.

212 EDF and AREVA claim that loss of either one emergency supplied switchboard or one regulated switchboard is bounded by the loss of one 10 kV AC switchboard from which they are supplied while loss of one 220 V DC switchboard does not result in any transient providing the 400 V AC UPS switchboard in the same division remains available. EDF and AREVA further argue (Ref. 16) that the loss of one 10 kV AC switchboard bounds the loss of one 690 kV AC switchboard both in terms of consequence (as the Class 2 UDGs cannot be claimed for PCC analysis) and frequency. In order to make this argument bounding it is necessary to assume that the timescales for consequential failure of the C&I and electrical equipment (which are powered by the UPS switchboards) that occur as a result of the loss of the safeguard building HVAC systems are calculated using the heat loads resulting from loss of only the 690 V AC switchboards. This is because the current design of the essential electrical system exclusively provides electrical power supplies to the HVAC systems from the 690 V AC switchboards. EDF and AREVA estimate that the timescale of loss of C&I and electrical systems following loss of the 690 V AC switchboard is 30 minutes based on FA3 studies that have not been shared with ONR. This increases to between 1 hour and 2 hours for the loss of one 10 kV AC switchboard. I have raised Assessment Finding **AF-UKEPR-FS-108** for a future licensee to confirm these timescales for the UK EPR™ during the site specific detailed design phase.

213 In addition, EDF and AREVA identify the following faults within this category that they consider to be the limiting common mode failures (Ref. 16):

- Total loss of supplies from the 10 kV AC (LH) switchboards.
- Total loss of supplies from the 690 V AC (LJ) switchboards.
- Total loss of supplies from the 400 V AC (LV) UPS switchboards.
- Total loss of supplies from the emergency supplied 400 V AC (LL) switchboards.
- Total loss of supplies from the regulated 230/400 V AC (LO) switchboards.
- Total loss of supplies from the 220 V DC (LA) UPS switchboards.

214 EDF and AREVA claim that loss of either the emergency supplied switchboards or the regulated switchboards is bounded by the loss of the 10 kV AC switchboards from which they are supplied while loss of the 220 V DC switchboards does not result in any transient providing the 400 V AC UPS switchboards remain available. This leaves the total loss of the 10 kV AC, 690 V AC and 400 V AC voltage levels to be reviewed as possible design basis events.

215 In the sections below, I have separately presented my assessment of partial failure of an essential electrical system (Section 4.6.2.1) from my assessment of total failure of an essential electrical system (Section 4.6.2.2).

4.6.2.1 Partial Loss of an Essential Electrical System

System Description of Essential Electrical Systems

216 Before reviewing the fault sequence analysis for this fault it is worth reviewing the system design for the nuclear island essential electrical systems.

217 The essential electrical system is divided into four independent electrical divisions that are each housed in one of the safeguard buildings. Each division is backed-up by an EDG. Each of these divisions is further sub-divided into four sub-divisions that provide the following functions:

- Emergency power supply for all the safety related loads from the EDGs and also in some cases on Divisions 1 and 4 from the UDGs.
- An Uninterruptible Power Supply (UPS) to support all the C&I systems, control for electrical switchboards, and other loads which must remain live before the start-up of the EDGs or UDGs. A dual supply is provided.
- A severe accident dedicated UPS that supports the management of severe accidents in the event of LOOP together with loss of all on-site emergency power.
- A dedicated power supply for the control rod mechanisms.

218 The provision of emergency power supply to the main loads differs between divisions. From the single line diagram of the essential electrical system (Ref. 32) it is clear that Divisions 1 and 4 are largely identical apart from the supplies provided to the FPCS. Division 1 supplies the 3rd train of FPCS while Division 4 supplies one of the main FPCS trains. Likewise, Divisions 2 and 3 are largely identical apart from the supplies provided to the FPCS. Division 2 supplies the other main FPCS train while Division 3 does not supply the FPCS. The main difference between Divisions 1 and 4 and Divisions 2 and 3 is that the UDGs provide a diverse source of emergency power supplies to the 690 V AC switchboards on Divisions 1 and 4 and so the safety related loads are re-arranged to take advantage. Given the fundamental symmetry in the design the allocation of the main safety related loads is therefore only described for Divisions 1 and 2.

219 In Division 1, the 10 kV AC switchboards supply the following safety related loads:

- ESWS train 1
- CCWS train 1
- MHSI train 1
- RCP number 1
- CVCS train 1 (of 2)
- Operational chilled water system

220 In Division 1, the 690 V AC switchboards supply the following safety related loads:

- UCWS train 1
- CHRS train 1
- LHSI train 1
- EFWS train 1
- EBS train 1 (of 2)

- FPCS train 3
- Safeguard building main HVAC system – train 1
- MCR HVAC train 1

221 In Division 2, the 10 kV AC switchboards supply the following safety related loads:

- ESWS train 2
- CCWS train 2
- MHSI train 2
- EFWS train 2
- RCP number 2

222 In Division 2, the 690 V AC switchboards supply the following safety related loads:

- LHSI train 2
- FPCS train 1 (of 2)
- Safeguard building main HVAC system – train 2
- MCR HVAC train 2

223 As the essential electrical system is a Class 1 system it is designed to meet the single failure criteria and is seismically qualified. EDF and AREVA claim that the design has taken account of internal and external hazards.

Fault Sequence Analysis

224 EDF and AREVA have treated the loss of a 10 kV AC switchboard listed above as a design basis fault meeting the requirements of FA.4 and FA.5 although they have not formally allocated it to be a PCC event within the PCSR but as "specific studies". I therefore consider that Assessment Finding **AF-UKEPR-FS-90**, which requires a future licensee to include such events within the design basis analysis of a site specific PCSR, to be equally applicable to the partial loss of essential electrical system fault as well. However, as with the loss of cooling chain faults and the loss of safeguard building main HVAC system faults, I recognise that the deterministic assessment performed does assume the most onerous single failure and the worst plant maintenance together with consequential LOOP following reactor trip so my judgement is that in practice the requirements of SAPs FA.6, EDR.2 and EDR.4 analysis rules are being met although the radiological assessment still has to be presented. In addition to the deterministic assessment and as part of the site specific detailed design phase, it will also be necessary to model loss of the essential electrical system faults within the PSA to confirm that the balance of risk is ALARP when judged against SAPs T.8 and T.9. I therefore consider that Assessment Finding **AF-UKEPR-FS-91**, which requires a future licensee to perform such an assessment, is equally applicable to these faults.

225 EDF and AREVA state (Refs 16 and 18) that the initiating frequency for loss of one 10 kV AC switchboard of the essential electrical system is 2×10^{-2} per year. EDF and AREVA therefore acknowledge that this event is a frequent fault. For this reason, they have performed a diversity analysis for common mode failure of frontline systems on demand in coincidence with these initiating events (Ref. 21) which I have assessed in my close-out report (Ref. 25) for Action 8 of GDA Issue **GI-UKEPR-FS-02** on functional diversity for frequent faults.

226 EDF and AREVA have performed a deterministic assessment (Refs 13 and 16) to establish the consequences of this single failure fault when coupled with the assumption of the most onerous single failure, the worst plant maintenance condition, and a consequential LOOP. As with the loss of cooling chain fault and the loss of safeguard building main HVAC system fault assessed in Sections 4.1.2.1 and 4.2.2.1 above, in my judgement, the approach is systematic and comprehensive. For each initiating fault, a series of tables are completed in which the most onerous single failure and plant maintenance are analysed from the same lists as before together with the assumption of LOOP.

227 Some general characteristics can be noted. The loss of a 10 kV AC switchboard fault is the most onerous of the single failure faults in the essential support systems identified by EDF and AREVA. This is because the initiating event results in the loss of one safeguard division as well as a reactor trip that is assumed to cause a consequential LOOP. Assuming the loss of two EDGs due to single failure and plant maintenance in coincidence with LOOP removes a further two safeguard divisions leaving just one safeguard division to protect against the fault. In contrast, the partial loss of cooling chain faults considered in Section 4.1.2.1 and partial loss of electrical systems considered in Section 4.6.2.1 are slightly less onerous. The design basis faults identified below which assume that only one safeguard division remains available are therefore appropriate for this partial loss of essential electrical system fault.

228 As before, depending upon which single failures and plant maintenance states are considered it is possible for a seal LOCA to occur on the four RCPs and for both EBS trains to be lost for intact circuit sequences.

229 In developing the safety case EDF and AREVA have not identified the need for any additional design changes to the essential electrical system to ensure compliance with the design basis analysis rules. However, the design modifications proposed under CMF#39, 41, 42, 75, and 76 (Ref. 8) and already assessed in earlier sections are claimed and are equally applicable for the partial loss of the essential electrical system.

230 As a result of the fault sequence analysis, which assumes the above modifications are in place, EDF and AREVA conclude (Refs 13 and 16) that for the reactor the same design basis faults bound these fault sequences as the partial loss of cooling chain faults and the partial loss of HVAC system faults discussed in Sections 4.1.2.1 and 4.2.2.1.above respectively. These are the following faults:

- Two tripped RCPs with loss of three safeguard building divisions.
- Four RCP seal LOCAs with loss of three safeguard building divisions.

231 I agree with this conclusion providing the proposed modifications discussed above and covered by Assessment Findings **AF-UKEPR-CC-01** and Assessment Findings **AF-UKEPR-FS-94**, **AF-UKEPR-FS-95** and **AF-UKEPR-FS-101** are fully implemented. I therefore judged that the functional analysis performed by EDF and AREVA to identify these sequences meets the requirements of SAPs FA.6, EDR.2 and EDR.4.

Transient Analysis

232 The limiting design basis events defined above are the same as those covering the partial loss of cooling chain system faults and the partial loss of safeguard building main HVAC system faults discussed in Sections 4.1.2.1 and 4.2.2.1 above. Hence the transient analysis studies (Ref. 15) that I have already assessed in Section 4.1.2.1 above are

equally applicable for partial loss of essential electrical system faults. Hence, in my judgement the requirements of SAP FA.7 are met for these faults as well.

4.6.2.2 Total Loss of an Essential Electrical System

Fault Sequence Analysis

233 The PCC analysis rules of EDF and AREVA do not apply to faults caused by a common mode failure. During GDA, there was an agreement between ONR, EDF and AREVA on the list of common cause failures to be considered within the essential electrical systems for the design basis analysis for the purposes of GDA (Refs 16, 18 and 33) and so EDF and AREVA have performed a design basis analysis for this fault consistent with UK practice (Ref. 7). In my judgement, this approach meets the requirements of SAPs FA.4 and FA.5.

234 In developing the safety case EDF and AREVA have proactively identified the need for a number of design changes generally associated with re-allocating the distribution of electrical loads on the essential electrical systems under CMF#78.

235 CMF#78 (Ref. 8) covers the following design changes:

- Re-allocation of the electrical supplies of the CCWS common isolation valves on trains 1 and 4 to the 220 V DC essential electrical system.
- Re-allocation of the electrical supplies of the ESWS heat exchanger regulation valves on trains 1 and 4 to the 220 V DC essential electrical system.
- Re-allocation of one of the three common isolation valves on each train of the SG blowdown system to the 220 V DC essential electrical system.
- Potential re-allocation of the CVCS actuators to maintain RCP seal injection.
- Re-allocation of the electrical supplies of one of the two pumps on each train of the FPCS to the 400 V AC essential electrical system.
- Re-allocation of the electrical supplies of the safeguard building diverse HVAC system chilled water trains 1 and 4 to the 400 V AC essential electrical system.
- Consideration of introducing additional manufacturing diversity across the divisions for the key active electrical components if necessary depending on the reliability of the claim.

236 In addition, CMF#37 (Ref. 8), covering the upgrade of the UDGs to Class 2, is also relevant as it provides a diverse electrical supplies to the 690 V AC essential electrical system.

237 Although design change proposal CMF#78 is covered by the generic Assessment Finding **AF-UKEPR-CC-05** clearly the proposed design changes are at a preliminary stage of development. In my judgement, given the potential implications to plant layout of these changes, it is essential that this analysis and design work is substantially completed early in the site specific detailed design phase. I have therefore raised Assessment Finding **AF-UKEPR-FS-109** for a future licensee to further develop these design change proposals prior to the pouring of Nuclear Island safety-related concrete.

238 Given the potential complexity of the functional analysis involved for a common mode failure assessment of the essential electrical system an agreement was reached between EDF and AREVA and the ONR, that for the purposes of GDA, the scope of the functional

analysis would be limited (Ref. 33). This was in recognition that the detailed design of the essential electrical system is still under development and that further studies would need to be performed during the site specific detail design phase. The agreement (Ref. 33) also covers the common mode failure cut-off frequencies to be assumed in future updates to the PSA. The proposed frequencies are based upon engineering judgement and have been assessed by ONR's electrical engineering specialists (Ref. 12) as acceptable.

239 The agreed scope of the study (Ref. 33) was that for GDA only common mode failure of either the 690 V or the 400 V voltage levels with the reactor at power would initially be considered. Claims would only be made on safety classified equipment. Only the first 12 hours corresponding approximately to the controlled state would need to be considered for the purposes of GDA. Within this scope, the aim of the EDF and AREVA analysis is to demonstrate that the controlled state can be reached with decay heat removal by the steam generators and that boiling of the spent fuel pool can be avoided.

240 In my judgement, while the limited scope of the review is adequate for the purposes of GDA in order to explore the design implications for the UK EPR™, there is a need to complete the review to a sufficient level of detail to give good confidence in plant layout prior to the pouring of Nuclear Island safety-related concrete. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-110** for a future licensee to complete the review covering common mode failure of other voltage levels, other safety functions such as feed and bleed and other plant states and to formally produce a safety case covering the analysis. To aid ONR's assessment it would also be helpful to be provided with a definitive list of electrical loads on all switchboards of the essential electrical system. I have therefore raised Assessment Finding **AF-UKEPR-FS-111** for a future licensee to provide as full a list as possible of the loads on the switchboards.

241 As noted above, the total loss of common voltage levels needs to be considered for the following three bounding events:

- Total loss of supplies from the 10 kV AC (LH) switchboards.
- Total loss of supplies from the 690 V AC (LJ) switchboards.
- Total loss of supplies from the 400 V AC (LV) UPS switchboards.

242 Each of these design basis events is reviewed in turn in the following paragraphs.

Total loss of the 10 kV AC voltage level

243 EDF and AREVA argue (Ref. 16) that this transient is bounded by the existing RRC-A SBO sequence (LOOP together with loss of EDGs) resulting in loss of the 10 kV supply. EDF and AREVA argue that provision is made in the design against SBO to ensure the safety functions are achieved and so no further analysis is required. However, this design provision includes a claim on the SSSS which is the equivalent of a Class 3 system to ensure the primary circuit remains intact. In particular, the SSSS is vulnerable to a single failure since it is a 4-out-of-4 system. If one of the valves on the SSSS fails to isolate then a seal LOCA will occur. The operator needs to start the UDGs so as to supply electrical power to the EFWS to remove decay heat and to the LHSI pumps to provide make-up following manual depressurisation of the primary system. The CHRS and UCWS can be used to cool the IRWST to ensure the continued operation of the LHSI. The LHSI also provides for the long term control of reactivity.

244 In my close-out report for Action 9 of GDA issue **GI-UKEPR-FS-02**, I have raised Assessment Finding **AF-UKEPR-FS-46** for a future licensee to provide a fully integrated

case for the SBO sequence. Nevertheless, I consider it essential that, in the interim, transient analysis studies are performed for this sequence to confirm that sufficient grace time exists for the operator to perform all these actions so as to avoid fuel damage. In addition, as only two EFWS pumps are available to remove decay heat and there is a delay before they start to operate, this sequence may possibly be more onerous in terms of the performance and sizing of the CHRS than the SBLOCA with loss of LHSI sequence and the total loss of cooling chain sequences discussed in Section 4.1.2.2 above. I have therefore raised Assessment Finding **AF-UKEPR-FS-112** for a future licensee to perform UK EPR™ specific transient analysis studies for the SBO sequence with failure of the SSSS. Given the potential implications on plant layout of these studies it is important that Assessment Finding **AF-UKEPR-FS-112** is resolved early in the site specific detailed design phase and prior to the pouring of Nuclear Island safety-related concrete.

245 A further issue is that during the assessment of the response of EDF and AREVA to GDA issue **GI-UKEPR-CC-03** on the lessons learnt from Fukushima (see Table 5, Ref. 31) it became apparent that EBS is not claimed for SBO sequences even though it is supplied from the 690 V AC switchboards in Divisions 1 and 4 that are backed-up by the UDGs. It is noted that there are a lot of other safety-related loads fed from these switchboards including the EFWS, LHSI, UCWS, CHRS, the 3rd train of the FPCS and the safeguard building main HVAC system. It is not clear why EDF and AREVA chose to shed the EBS load. It may be that the UDGs do not have sufficient capacity to supply all these loads. Although there appears to be sufficient systems available (Ref. 31) to ensure long term reactivity control using a bleed and feed operation, it is desirable from a safety perspective to maximise the availability of plant in this situation. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-113** for a future licensee to confirm which loads the UDG is functionally capable of supplying concurrently from these switchboards.

Total loss of the 690 V AC voltage level

246 EDF and AREVA have performed a functional analysis to establish the consequences following total loss of the 690 V AC voltage level with the reactor at power. The analysis claims the modifications that are proposed under CMF#41 on the safeguard building diverse HVAC system, CMF#42 and CMF#76 on the cooling chain systems, CMF#77 on the MCR HVAC system, and CMF#78 on the essential electrical systems discussed earlier. The modification CMF#78 is particularly important as it ensures that the safeguard building diverse HVAC system remains available to cool the C&I and electrical equipment in the safeguard buildings. EDF and AREVA are exploring whether it might be possible to cool all four safeguard divisions given the lower heat loads as a consequence of loss of the 690 V AC voltage levels. This will be confirmed during the site specific detailed design phase. With these modifications in place two EFWS and four divisions of MSRTs remain available to cool the reactor following manual reactor trip. Cooling of the thermal barriers is ensured by trains 1 and 4 of the CCWS that are supplied from the 10 kV AC switchboards. In my judgement, an acceptable solution has been proposed by EDF and AREVA to cover the total loss of the 690 V AC voltage level for the purposes of GDA recognising that the solution will be explored further during the site specific detailed design phase and that other solutions may emerge during this phase.

247 In particular, for the purposes of GDA, I judged it necessary to ensure that the controlled state could be reached following total loss of the 690 V AC voltage level. For this reason, I agreed that the scope of the study could be limited to the first 12 hours of the fault transient. Nevertheless, it is highly desirable from a safety perspective to be able to ensure the long term control of reactivity without having to claim the operator restore /

repair of the lost voltage level as the common mode failure mechanism may be complex. With the loss of 690 V AC voltage level both EBS trains will become unavailable. Given that there are only two EBS trains and EDF and AREVA are proposing that these will be cross-connected to their adjacent electrical division when maintenance is performed on their own electrical divisions, I can understand why EDF and AREVA will not want to alter the supply voltage for the EBS. Nevertheless, given that all the MHSI pumps are fed from the 10 kV AC voltage level, a bleed and feed operation would ensure control of reactivity providing the primary circuit can be manually depressurised. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-114** for a future licensee to explore whether long term control of reactivity can be assured.

248 It is noted that as a result of CMF#78 the safeguard building diverse HVAC system and two of the main FPCS pumps, one from each train, will be supplied from the 400 V AC switchboards. These changes protect these systems against common mode failure on the 690 V AC voltage level. However, they do not protect the safeguard building diverse HVAC system from total loss of all AC power supplies. This is significant since the UPS will ensure that in these circumstances the C&I systems including those associated with the essential electrical system will remain powered even though the HVAC systems that cool them will have failed. EDF and AREVA argue that on the basis of thermal analysis performed for FA3 that the thermal inertia of the safeguard building is sufficient to ensure that the C&I systems will not fail prior to the restoration of AC power supplies to the HVAC systems (Ref. 16). However, this analysis has not been shared with ONR. I have therefore raised Assessment Finding **AF-UKEPR-FS-115** for a future licensee to perform thermal analysis to determine the timescales for which consequential loss of C&I and electrical equipment would occur as a result of the total loss of all the HVAC systems during the station blackout sequence prior to restoration of the UDGs. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative destructive testing. I have also raised the related Assessment Finding **AF-UKEPR-FS-116** for a future licensee to perform thermal analysis to confirm that the C&I and electrical equipment needed to operate the severe accident mitigation measures will remain available despite the complete loss of all HVAC systems following the severe accident sequence associated with station blackout occurring together with subsequent failure of the UDGs to start. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative testing.

Total loss of the 400 V AC UPS voltage level

249 EDF and AREVA have performed a functional analysis to establish the consequences following total loss of the 400 V AC voltage level with the reactor at power. The analysis claims the modifications that are proposed under CMF#78 on the essential electrical systems. The significant design change is that some redundant valve actuations have been moved from the 400 V AC UPS to the 220 V DC UPS. With these modifications in place four EFWS trains remain available to cool the reactor following automatic reactor trip. Cooling of the thermal barriers is ensured by trains 1 and 4 of the CCWS that are supplied from the 10 kV AC switchboards. In my judgement, an acceptable solution has again been proposed by EDF and AREVA to cover the total loss of the 400 V AC voltage level for the purposes of GDA recognising that the solution will be explored further during the site specific detailed design phase and that other solutions may emerge during this phase. As with the previous case, it is desirable that a bleed and feed capability should also be demonstrated if possible.

250 In summary, recognising that the UK EPR™ is an "all electric" design it is important that the essential electrical system incorporates as much diversity as possible to improve its reliability as required by SAP EDR.3. As a result of the proposed modifications, EDF and AREVA have considerably improved the robustness of the essential electrical system with regard to the effect of a total failure of identical voltage levels. The situation is a little analogous to the design of the Heysham 2 and Torness AGR stations where the electrical supplies are not only divided into four electrical divisions that are physically located in different quadrants but are also grouped into two diverse sub-systems based upon different voltage levels called the X and Y trains. The UK EPR™ is now very similar to this concept in that the main safety loads are segregated between the 10 kV and 400 V AC supplies and the 690 V AC supplies while the C&I equipment and mechanical valve actuators are segregated between the 400 V AC and 220 V DC supplies. The use of diverse DC and AC electrical supplies also ensures that the valve actuators themselves will be of a diverse design. There is still further work to be performed during the site specific detailed design phase but in my judgement sufficient progress has been made for the purposes of GDA to justify closure of GDA issue **GI-UKEPR-FS-05** with regard to the essential electrical system. This is subject to completion of the modifications and analysis covered by Assessment Findings **AF-UKEPR-FS-109** to **AF-UKEPR-FS-116**.

4.6.3 Findings

251 Following my assessment of the EDF and AREVA submissions, I am content for GDA issue **GI-UKEPR-FS-05** to be closed with regard to the essential electrical system. Assessment Findings **AF-UKEPR-FS-109** to **AF-UKEPR-FS-116** have been raised.

4.7 Review of the Updates to the PCSR

252 Chapters 3.2, 6.6, 9.2, 9.4, 14.7, 16.4 and 18.2 of the updated PCSR (Ref. 22) present the safety case for loss of essential support systems. In particular, Chapter 16.4 provides an overall summary of the safety case. These chapters have been reviewed to ensure that the outcome of the GDA assessment has been appropriately captured within the PCSR. I am satisfied that the revised chapters accurately reflect the safety case arguments, transient analysis studies and design modifications developed to justify the closure of **GI-UKEPR-FS-05.**

253 While the PCSR accurately reflects the current position of the safety case it does this by cross referencing from Chapters 6.6, 9.2 and 9.4 to Chapter 16.4. Clearly, there is a need at a further update to site specific PCSR to rationalise the presentation of the safety case. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-117** for a future licensee to better integrate the loss of essential support systems safety case into the site specific PCSR.

254 I note that in Chapter 16.4 the safety classification of the SSSS is stated as Class 2. In the FA3 design this is an F2 feature which equates to Class 3. There is therefore a need to justify that the SSSS meets the requirements of a Class 2 system. However, I consider that this demonstration can be performed as part of the response to cross-cutting Assessment Finding **AF-UKEPR-CC-05** on application of the UK categorisation and classification methodology to the UK EPR™ design.

255 In performing my assessment of the updates, I became aware of the following areas that need to be updated in future updates to the site specific PCSR:

- Section 6.2.3.3 of Chapter 18.2 states that preventive maintenance of the CHRS and SBO (UDGs) diesel generators is possible while the unit is in operation. From the wording it is unclear whether this means both trains of the CHRS and the UDGs can be inoperable at the same time or only a single train. For this reason, I am raising Assessment Findings **AF-UKEPR-FS-118** and **AF-UKEPR-FS-119** for a future licensee to confirm that planned periodic maintenance will only be performed on a single train of these systems at a time.
- I welcome the fact that Section 4.4.2 of Chapter 18.2 has been updated to reference the analysis (Ref. 34) which establishes the neutronic design Safety Analysis Bounding Limit (SABL) requirements. I have reviewed this analysis and consider that it is adequate for the purposes of GDA. However, in my judgement there is a need for an additional SABL to be added to cover the fission gas pressure distribution assumed in the fuel rods as a function of burn-up. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-120** for a future licensee to include the assumed fission gas pressure distribution as a function of burn-up as a SABL.

256 In addition, there is a general need to update site specific versions of the PCSR to reflect the UK categorisation and classification scheme. I expect this update to be performed under the cross-cutting Assessment Finding **AF-UKEPR-CC-05**.

5 ASSESSMENT CONCLUSIONS

257 EDF and AREVA have undertaken a large amount of analysis work within the Fault Studies assessment area during the close-out phase of GDA and made significant progress against GDA Issue **GI-UKEPR-FS-05** covering the loss of essential support system faults identified in my GDA Step 4 assessment report.

258 In my opinion, EDF and AREVA have considerably strengthened the design basis safety case against loss of essential support system faults for the UK EPR™ through the additional safety case analysis performed in response to GDA Issue **GI-UKEPR-FS-05**. This has included systematically reviewing the consequences of single failures and common mode failures on each of the essential support systems. The work has been supported by the performance of additional transient analysis studies to demonstrate that sufficient front line systems remain available to reach the safe shutdown state following such failures.

259 The analytical work performed by EDF and AREVA has been aided by a number of important design changes to the essential support 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 changes identified are (in order of assessment in this report):

- Upgrade of the automatic switchover from the operating CCWS / ESWS train to the stand-by CCWS / ESWS train on loss of the operating train to Class 1.
- Upgrade of the automatic isolation of the operating CCWS / ESWS train from the common auxiliaries header in case of leakage to Class 1.
- Upgrade of the automatic trip on the Reactor Coolant Pumps (RCP) on low injection flow rate to the seals or high thermal barrier temperature to Class 1.
- Upgrade of the automatic switchover of the cooling of the Low Head Safety Injection (LHSI) pumps 1 and 4 from the CCWS to the safeguard building ventilation system on low CCWS flow rate or high CCWS temperature to Class 1.
- Upgrade of the manual realignment of the Emergency Feedwater System (EFWS) common pump discharge headers from a local to plant action to a main control room action at Class 1.
- Addition of a common header on the CCWS lines cooling the Reactor Coolant Pump (RCP) thermal barriers.
- Upgrade of the safeguard building chilled water system to Class 1.
- Upgrade of the safeguard building ventilation system to Class 1.
- Creation of a new Class 2 safeguard building diverse chilled water system allocated to divisions 1 and 4 of the 400V AC essential electrical system that will be housed in an extra single storey to be added to safeguard buildings 1 and 4.
- Creation of a new Class 1 safeguard building diverse ventilation system allocated to divisions 1 and 4 of the 400V AC essential electrical system.
- Upgrade of the automatic switchover from the safeguard building ventilation system to the safeguard building new diverse ventilation system on loss of normal systems to Class 1.

- Upgrade of the automatic switchover from the safeguard building chilled water system to the safeguard building new diverse chilled water system on loss of normal systems to Class 2.
- Upgrade of the main control room air conditioning system to Class 1.
- Upgrade of the high temperature alarms in the ESWS shaft of the pumping station to Class 1.
- Implementation of a back-up electrical supply to the Extra Boration System (EBS) trains and associated C&I and support systems.
- A reallocation of the electrical supplies of the CCWS common isolation valves on trains 1 and 4 to the 220V DC essential electrical system.
- A reallocation of the electrical supplies of the ESWS heat exchanger regulation valves on trains 1 and 4 to the 220V DC essential electrical system.
- A reallocation of the electrical supplies for one of the common isolation valves on each train of the steam generator blowdown system to the 220V DC essential electrical system.
- A reallocation of the electrical supplies of one of the two pumps on each train of the Fuel Pool Cooling System (FPCS) to the 400V AC essential electrical system.
- A reallocation of the electrical supplies of the safeguard building diverse chilled water system to the 400V AC essential electrical system.

260 In my judgement any additional design changes that may result from the closure of Assessment Findings are likely to be limited to changes in the allocation of electrical loads in two out of the four electrical divisions in the safeguard buildings and changes in the C&I control systems for the HVAC systems. Given the potential implications to plant layout of these changes, it is considered essential that this analysis and design work is substantially completed early in the site specific detailed design phase and prior to the issue of Consent to start the pouring of Nuclear Island safety-related concrete.

5.1 Overall Conclusions

261 Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that sufficient progress has been made on the safety case for loss of essential support system faults presented in the supporting documentation submitted in response to GDA Issue **GI-UKEPR-FS-05** to justify its closure subject to satisfactory progression and resolution of the Assessment Findings identified in Annex 2. These are to be addressed during the forward work programme for this reactor. For this reason, I am satisfied that GDA issue **GI-UKEPR-FS-05** can now be closed.

6 ASSESSMENT FINDINGS

6.1 Additional Assessment Findings

262 The following Assessment Findings have been raised that are required to be resolved during the site specific detailed design phase:

AF-UKEPR-FS-90: *The future licensee shall allocate single loss of essential support systems as design basis faults within the PCSR.*

Required timescale: *Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site*

AF-UKEPR-FS-91: *The future licensee shall update the PSA for UK EPR™ to adequately cover loss of essential support system faults including all the modifications developed in response to GI-UKEPR-FS-05.*

Required timescale: *Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site*

AF-UKEPR-FS-92: *The future licensee shall review the adequacy of the design basis analysis rules for spent fuel faults to take account of the likelihood of consequential LOOP following loss of essential support system faults.*

Required timescale: *Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site*

AF-UKEPR-FS-93: *The future licensee shall confirm that the design modifications proposed under CMF#42 meet the single failure criteria.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-94: *The future licensee shall develop the design changes to cooling chain systems proposed under CMF#75 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-95: *The future licensee shall provide full justification for the modification proposed in CMF#76 to add a common header between the CCWS thermal barrier cooling systems lines. In particular, a demonstration shall be provided that a break in the line does not introduce any significant safety dis-benefits. Further justification is also required on the reason for selecting the chosen option over the other ALARP options that were rejected.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-96: *The future licensee shall develop the design changes identified in the total loss of cooling chain analysis under CMF#79 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-97: *The future licensee shall perform UK EPR™ specific transient analysis studies to confirm that the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to*

the IRWST following total loss of cooling chain fault for states in which maintenance of the CHRS is allowed.

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-98: *The future licensee shall perform UK EPR™ specific transient analysis studies to confirm whether the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to the IRWST following the SBLOCA fault with failure of LHSI or to demonstrate that the current design of the CHRS is ALARP.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-99: *The future licensee shall confirm that the diverse intake lines of the UCWS are sized sufficiently such that one UCWS train is functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state A and that two UCWS trains are functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state D.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-100: *The future licensee shall perform UK EPR™ specific transient analysis studies to confirm that the CHRS is sized sufficiently such that two CHRS trains are functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state D and that adequate grace time is available for operator action.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-101: *The future licensee shall develop the conceptual design for the safeguard building main HVAC systems proposed under CMF#41 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems. This needs to demonstrate that mechanical diversity has been achieved between trains 1 and 4 and trains 2 and 3 as well as with the safeguard building diverse HVAC system. It also needs to demonstrate that the ventilation trains of the safeguard building main HVAC can provide adequate cooling following failure of their associated chilled water train**.***

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-102: *The future licensee shall develop the design changes for the main control room HVAC system proposed under CMF#77 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems and review the safety classification of the remote shutdown station HVAC system.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-103: *The future licensee shall review the design of the operational chilled water system to confirm that the likelihood of common mode failure has been reduced to ALARP.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-104: *The future licensee shall determine the consequences of failure for the control rod drive mechanisms and the ex-core flux instrumentation of the containment cooling ventilation system.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-105: *The future licensee shall perform thermal analysis to confirm that the UCWS is able to function continuously on demand following loss of the CW pump house HVAC system.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-106: *The future licensee shall develop the design changes for the circulation water pump house HVAC system proposed under CMF#80 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-107: *The future licensee shall perform thermal analysis to confirm that the EFWS and LHSI are able to function continuously on demand following loss of HVAC cooling to their pump rooms.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-108: *The future licensee shall perform thermal analysis to confirm the timescales for consequential loss of C&I and electrical equipment following loss of a safeguard building HVAC train due to failure of its supply from a) the 690 V switchboard and b) the 10 kV switchboard.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-109: *The future licensee shall develop the design changes to essential electrical systems proposed under CMF#78 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-110: *The future licensee shall continue to review the allocation of electrical loads to the essential electrical system for those systems and safety functions not reviewed in the current safety case to ensure that the optimum distribution is achieved to reduce the risks from common mode failure to as low as reasonably practicable. The review should include the bleed and feed function, other plant states, and the loss of other voltage levels including the 10 kV voltage level.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-111: *The future licensee shall provide as full a list as possible of all the electrical loads on each switchboard of the essential electrical system.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-112: *The future licensee shall perform UK EPR™ specific transient analysis studies for the SBO sequence with failure of the SSSS. The analysis will need to confirm that adequate grace time is available for operator action to start the UDGs and restore adequate cooling and whether the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to the IRWST or to demonstrate that the current design of the CHRS is ALARP.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-113: *The future licensee shall confirm that the UDGs are sized sufficiently that each one can simultaneously power sufficient electrical loads on its associated 690V switchboards following the loss of the 10 kV voltage level to reach the safe shutdown state and cool the spent fuel pool subject to ALARP.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-114: *The future licensee shall demonstrate that the long term control of reactivity after 12 hours is assured following loss of the 690 V AC voltage level.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-115: *The future licensee shall perform thermal analysis to determine the timescales for which consequential loss of C&I and electrical equipment would occur as a result of the total loss of all the HVAC systems during the station blackout sequence prior to restoration of the UDGs. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative destructive testing.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-116: *The future licensee shall perform thermal analysis to confirm that the C&I and electrical equipment needed to operate the severe accident mitigation measures will remain available despite the complete loss of all HVAC systems following the severe accident sequence associated with station blackout occurring together with subsequent failure of the UDGs to start. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative testing.*

Required timescale: *Nuclear Island safety-related concrete*

AF-UKEPR-FS-117: *The future licensee shall update the PCSR to capture the revised safety case for loss of essential support systems.*

Required timescale: *Fuel to Site*

AF-UKEPR-FS-118: *The future licensee shall confirm that the technical specifications for control of availability of the CHRS will not allow planned maintenance to be performed on both trains of the CHRS at the same time.*

Required timescale: *Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site*

AF-UKEPR-FS-119: *The future licensee shall confirm that the technical specifications for control of availability of the UDGs will not allow planned maintenance to be performed on both trains of the UDGs at the same time.*

Required timescale: *Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site*

AF-UKEPR-FS-120: *The future licensee shall provide a safety analysis bounding limit (SABL) for fission gas pressure distribution as a function of burn-up for incorporation into the technical specifications.*

Required timescale: *Fuel to Site*

263 These Assessment Findings are listed in Annex 2.

6.1.1 Impacted Step 4 Assessment Findings

264 As noted in the main text of the report, two pre-existing Assessment Findings have been impacted as a result of this assessment. **AF-UKEPR-FS-08** requires the fault analysis be updated to reflect the UK EPR™ design. Similarly, **AF-UKEPR-FS-29** requires that the fault schedule in the PCSR is regularly updated to reflect revisions in the safety case. Assessment Finding **AF-UKEPR-FS-45** requires a future licensee to demonstrate that for frequent faults adequate functional diversity is provided in the essential support systems.

265 It is also noted that the generic cross cutting Assessment Finding **AF-UKEPR-CC-01** requires a future licensee to complete all the modifications identified during the GDA process while the generic cross cutting Assessment Finding **AF-UKEPR-CC-05** requires the UK categorisation and classification process to be applied to the UK EPR™. One of the requirements of this classification scheme is that systems that provide a diverse line of protection should have a safety classification of at least Class 2.

7 REFERENCES

1 *GDA Issue GI-UKEPR-FS-05 Revision 0. Design Basis Analysis of Essential Support Systems.* ONR. July 2011. TRIM Ref. 2011/385301.

2 *Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020a Revision 0. TRIM Ref. 2010/581404.

3 *Resolution Plan for GDA Issue GI-UKEPR-FS-05 Revision 0.* EDF and AREVA. June 2011. TRIM Ref. 2011/336354.

4 *ONR HOW2 Permissioning – Purpose and Scope of Permissioning.* PI/FWD Issue 3. HSE. August 2011.

5 *Assessment Plan for Fault Studies, Closure of GDA for the EPR™.* ONR-GDA-AP-11-007 Revision 0, October 2011. TRIM Ref. 2011/479495.

6 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.

7 *Technical Assessment Guide. Transient Analysis for Design Basis Accidents in Nuclear Reactors*. T/AST/034 Issue 1. HSE. Nov 1999.
Technical Assessment Guide. Validation of Computer Codes and Calculational Methods T/AST/042 Issue 1. HSE.
www.hse.gov.uk/nuclear/operational/tech_asst_guides/index.htm.

8 *Reference Design Configuration*. UKEPR-I-002 Revision 9. UK EPR. 26 October 2010. TRIM Ref. 2011/204075.

9 *EDF and AREVA UK EPR™ - Schedule of Technical Queries Raised during GDA Close-out.* Office for Nuclear Regulation. TRIM Ref. 2011/389411.

10 *PSA Assessment Note: Review of ENFCFI20092 and overview of electrical systems PSA,* Office for Nuclear Regulation August 2012, TRIM Ref. 2012/0304401.

11 *Electrical Engineering Assessment Report for GI-UKEPR-EE-01,* ONR Assessment Report ONR-GDA-AR-12-021 Revision 0 TRIM Ref. 2012/21.

12 *Assessment Note – Common Cause Failure on 400V AC LV and LJ switchboards on UK EPR™,* Office for Nuclear Regulation. March 2013, TRIM Ref. 2013/86340.

13 *Report A – Design Basis Analysis of single fault on essential support systems*, EDF and AREVA, ECESN120355, Rev A, June 2012, TRIM Ref. 2012/243787.

14 *Report B – Probabilistic assessment of the initiating events relative to the loss of DVL and DEL trains in the frame of the GDA issue GI-UKEPR-FS-05,* EDF and AREVA, ECESN120408, Rev A, June 2012, TRIM Ref. 2012/261769.

15 *Report C – Loss of support systems – Transient Analysis,* EDF and AREVA, PEPR-F DC 103, Rev B, October 2012, TRIM Ref. 2012/415845.

16 *Report D – GDA FS-05 – Faults in Essential Support Systems – ALARP Assessments, Proposed Design Changes and Justification of Resultant Design,* EDF and AREVA, ECESN0121088, Rev A, November 2012. TRIM Ref. 2012/461305.

17 *Report E – EPR™ UK GDA – GDA issue FS-05 – Safety frame for common cause failure events on the cooling chain, and analysis of classification upgrade of TLOCC mitigation means,* EDF and AREVA, PEPSDF/12.328, July 2012, TRIM Ref. 2012/298414.

18 *Report F – Identification of single and common modes of failure for the electrical systems for the UK EPR GDA issue FS-05,* EDF and AREVA, ENFCFI120092, Rev A, April 2012, TRIM Ref. 2012/243789.

19 *Report G –GDA – DVL / DEL – Conceptual design note,* EDF and AREVA, ECECS121567, Rev A, November 2012, TRIM Ref. 2012/439779.

20 *Report I – Screening of the HVAC systems to establish the impact of their loss on normal operation systems and on safety systems,* EDF and AREVA, ECESN120253, Rev A, October 2012, TRIM Ref. 2012/419759.

21 *Report J – Response to GI-UKEPR-FS-02 – Actions 8 and 9 – Diversity for frequent faults and to GI-UKEPR-FS-05 Action 1 – Loss of support systems,* Detailed in Letter EPR01281N, EDF and AREVA, July 2012, TRIM Ref. 2012/293524.

22 *PCSR Sub-Chapter 3.2 Update – Classification of structures, equipment and systems* UKEPR-0002-032 Issue 04, November 2012, TRIM Ref. 2012/472513.

PCSR Sub-Chapter 6.6 Update – Emergency Feedwater System (ASG) [EFWS] UKEPR-0002-066 Issue 04, November 2012, TRIM Ref. 2012/472546.

PCSR Sub-Chapter 9.2 Update – Water Systems
UKEPR-0002-092 Issue 04, November 2012, TRIM Ref. 2012/472576.

PCSR Sub-Chapter 9.4 Update – Heating, Ventilation and Air-Conditioning Systems
UKEPR-0002-094 Issue 03, November 2012, TRIM Ref. 2012/472578.

PCSR Sub-Chapter 14.7 Update – Fault and Protection Schedule
UKEPR-0002-149 Issue 03, November 2012, TRIM Ref. 2012/472435.

PCSR Sub-Chapter 16.4 Update – Specific Studies
UKEPR-0002-166 Issue 04, November 2012, TRIM Ref. 2012/467463.

PCSR Sub-Chapter 18.2 Update – Normal Operation
UKEPR-0002-182 Issue 06, November 2012, TRIM Ref. 2012/472500.

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

24 *UK EPR GDA Step 4 Consolidated Pre-construction Safety Report – March 2011.* EDF and AREVA. Detailed in EDF and AREVA letter UN REG EPR00997N. 18 November 2011. TRIM Ref. 2011/552663.

25 *Fault Studies Assessment Report for GI-UKEPR-FS-02,* ONR Assessment Report ONR-GDA-AR-12-011, Revision 0, TRIM Ref. 2012/11.

26 *Fault Studies Assessment Report for GI-UKEPR-FS-03,* ONR Assessment Report ONR-GDA-AR-12-012, Revision 0, TRIM Ref. 2012/12.

27 *Cross Cutting Assessment Report for GI-UKEPR-CC-01,* ONR Assessment Report ONR-GDA-AR-12-023 Revision 0 TRIM Ref. 2012/23.

28 *GDA Issue FS05 – TQ-1621 – partial answer to TQ,* EDF and AREVA, peprf12.1371, October 2012, TRIM Ref. 2012/401815.

29 *System Design Manual for CCWS:*
DSE RRI P3 – System and Component Dimensioning, EDF and AREVA, SFL-EF-MF-2006-416, August 2008, TRIM Ref. 2011/94342.

30 *System Design Manual for CHRS:*
Containment heat removal system EVU (CHRS) Plant System File: P3 – System Design, EDF and AREVA, SFL-EF-MF-2006-694, July 2008, TRIM Ref. 2012/155408.

31 *UK EPR GDA Project – Robustness of Power Sources/Long Term Cooling,* EDF and AREVA, PEPSF DC 133, Rev C, November 2012, TRIM Ref. 2012/449735.

32 *UK Project Single Line Diagram Nuclear Island Conventional Island,* EDF and AREVA, EDTOFC/080299, Rev B, May 2009, TRIM Ref. 2012/216143.

33 *GI-UKEPR-FS-05 – Summary of Conclusions from Fault Studies Level 4 meeting on Common Cause Failure of electrical systems (LV and LJ),* EDF and AREVA, Letter EPR01463R, 23rd November 2012, TRIM Ref. 2012/461348.

34 *UK EPR GDA – Neutronic Design Safety Analysis Bounding Limits,* EDF and AREVA, PEPCF.10.1041, Rev 3, December 2010, TRIM Ref. 2011/86026.

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-05 Revision 0 – Design Basis Analysis for Essential Support Systems – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Area	Document Ref.	Title	Ref.
UK-UKEPR-FS-05.A1	Functional Analysis of partial loss (single failures) of essential support systems	ECESN120355 Rev A	Report A – Design Basis Analysis of single fault on essential support systems	13
UK-UKEPR-FS-05.A1	Probabilistic Analysis of Safeguard Building HVAC systems	ECESN120408 Rev A	Report B – Probabilistic assessment of the initiating events relative to the loss of DVL and DEL trains in the frame of the GDA issue GI-UKEPR-FS-05	14
UK-UKEPR-FS-05.A1	Transient Analysis of partial loss (single failures) of essential support systems	PEPR-F DC 103 Rev B	Report C – Loss of support systems – Transient Analysis	15
UK-UKEPR-FS-05.A1	ALARP Review	ECESN121088 Rev A	Report D – GDA FS-05 – Faults in Essential Support Systems – ALARP Assessments, Proposed Design Changes and Justification of Resultant Design	16
UK-UKEPR-FS-05.A1	Functional analysis of complete loss of cooling chain (Total Loss of Cooling Chain - TLOCC)	PEPSDF/12.328 Rev 0	Report E – EPR™ UK GDA – GDA issue FS-05 – Safety frame for common cause failure events on the cooling chain, and analysis of classification upgrade of TLOCC mitigation means	17
UK-UKEPR-FS-05.A1	Probabilistic analysis of complete and partial loss of essential electrical systems initiating event frequencies	ENFCFI120092 Rev A	Report F – Identification of single and common modes of failure for the electrical systems for the UK EPR GDA issue FS-05	18
UK-UKEPR-FS-05.A1	Conceptual Design for Safeguard Building HVAC systems	ECECS121567 Rev A	Report G –GDA – DVL / DEL – Conceptual design note	19
UK-UKEPR-FS-05.A1	Functional Analysis of loss of other HVAC systems	ECESN120253 Rev A	Report I – Screening of the HVAC systems to establish the impact of their loss on normal operation systems and on safety systems	20

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-05 Revision 0 – Design Basis Analysis for Essential Support Systems – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Area	Document Ref.	Title	Ref.
UK-UKEPR-FS-05.A1	Functional Diversity for Frequent Faults	Letter EPR01281N	Report J – Response to GI-UKEPR-FS-02 – Actions 8 and 9 – Diversity for frequent faults and to GI-UKEPR-FS-05 Action 1 – Loss of support systems	21
UK-UKEPR-FS-05.A1	Transient Analysis of partial loss (single failures) of essential support systems	Peprf12.1371 Rev 0	GDA issue FS05 – TQ1621 – Partial answer to TQ	28
UK-UKEPR-FS-05.A1	Complete (CCF) failure of essential electrical voltage levels	Letter EPR01463R	GI-UKEPR-FS-05 – Summary of Conclusions from Fault Studies Level 4 meeting on Common Cause Failure of electrical systems (LV and LJ)	33

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-05 Revision 0 – Design Basis Analysis for Essential Support Systems – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1621	GI-UKEPR-FS-05.A1	ECESN120355 Rev A PEPR-F DC 103 Rev B	Loss of support systems

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-90	The future licensee shall allocate single loss of essential support systems as design basis faults within the PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-91	The future licensee shall update the PSA for UK EPR™ to adequately cover loss of essential support system faults including all the modifications developed in response to GI-UKEPR-FS-05.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-92	The future licensee shall review the adequacy of the design basis analysis rules for spent fuel faults to take account of the likelihood of consequential LOOP following loss of essential support system faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-93	The future licensee shall confirm that the design modifications proposed under CMF#42 meet the single failure criteria.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-94	The future licensee shall develop the design changes to cooling chain systems proposed under CMF#75 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-95	The future licensee shall provide full justification for the modification proposed in CMF#76 to add a common header between the CCWS thermal barrier cooling systems lines. In particular, a demonstration shall be provided that a break in the line does not introduce any significant safety dis-benefits. Further justification is also required on the reason for selecting the chosen option over the other ALARP options that were rejected.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-96	The future licensee shall develop the design changes identified in the total loss of cooling chain analysis under CMF#79 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.	Nuclear Island safety-related concrete.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-97	The future licensee shall perform UK EPR™ specific transient analysis studies to confirm that the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to the IRWST following total loss of cooling chain fault for states in which maintenance of the CHRS is allowed.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-98	The future licensee shall perform UK EPR™ specific transient analysis studies to confirm whether the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to the IRWST following the SBLOCA fault with failure of LHSI or to demonstrate that the current design of the CHRS is ALARP.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-99	The future licensee shall confirm that the diverse intake lines of the UCWS are sized sufficiently such that one UCWS train is functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state A and that two UCWS trains are functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state D.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-100	The future licensee shall perform UK EPR™ specific transient analysis studies to confirm that the CHRS is sized sufficiently such that two CHRS trains are functionally capable of providing adequate cooling to the IRWST following the loss of cooling chain fault in plant state D and that adequate grace time is available for operator action.	Nuclear Island safety-related concrete.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-101	The future licensee shall develop the conceptual design for the safeguard building main HVAC systems proposed under CMF#41 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems. This needs to demonstrate that mechanical diversity has been achieved between trains 1 and 4 and trains 2 and 3 as well as with the safeguard building diverse HVAC system. It also needs to demonstrate that the ventilation trains of the safeguard building main HVAC can provide adequate cooling following failure of their associated chilled water train.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-102	The future licensee shall develop the design changes for the main control room HVAC system proposed under CMF#77 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems and review the safety classification of the remote shutdown station HVAC system.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-103	The future licensee shall review the design of the operational chilled water system to confirm that the likelihood of common mode failure has been reduced to ALARP.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-104	The future licensee shall determine the consequences of failure for the control rod drive mechanisms and the ex-core flux instrumentation of the containment cooling ventilation system.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-105	The future licensee shall perform thermal analysis to confirm that the UCWS is able to function continuously on demand following loss of the CW pump house HVAC system.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-106	The future licensee shall develop the design changes for the circulation water pump house HVAC system proposed under CMF#80 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.	Nuclear Island safety-related concrete.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-107	The future licensee shall perform thermal analysis to confirm that the EFWS and LHSI are able to function continuously on demand following loss of HVAC cooling to their pump rooms.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-108	The future licensee shall perform thermal analysis to confirm the timescales for consequential loss of C&I and electrical equipment following loss of a safeguard building HVAC train due to failure of its supply from a) the 690 V switchboard and b) the 10 kV switchboard.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-109	The future licensee shall develop the design changes to essential electrical systems proposed under CMF#78 into a fully developed detailed design sufficient for a detailed specification of the requirements for the mechanical, electrical and C&I sub-systems.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-110	The future licensee shall continue to review the allocation of electrical loads to the essential electrical system for those systems, voltage levels and safety functions not reviewed in the current safety case to ensure that the optimum distribution is achieved to reduce the risks from common mode failure of different voltages to as low as reasonably practicable. The review should include the bleed and feed function, other plant states, and the loss of other voltage levels including the 10 kV voltage level.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-111	The future licensee shall provide as full a list as possible of all the electrical loads on each switchboard of the essential electrical system.	Nuclear Island safety-related concrete.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-112	The future licensee shall perform UK EPR™ specific transient analysis studies for the SBO sequence with failure of the SSSS. The analysis will need to confirm that adequate grace time is available for operator action to start the UDGs and restore adequate cooling and whether the CHRS is sized sufficiently such that one CHRS train is functionally capable of providing adequate cooling to the IRWST or demonstrate that the current design of the CHRS is ALARP.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-113	The future licensee shall confirm that the UDGs are sized sufficiently that each one can simultaneously power sufficient electrical loads on its associated 690V switchboards following the loss of the 10 kV voltage level to reach the safe shutdown state and cool the spent fuel pool subject to ALARP.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-114	The future licensee shall demonstrate that the long term control of reactivity after 12 hours is assured following loss of the 690 V AC voltage level.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-115	The future licensee shall perform thermal analysis to determine the timescales for which consequential loss of C&I and electrical equipment would occur as a result of the total loss of all the HVAC systems during the station blackout sequence prior to restoration of the UDGs. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative destructive testing.	Nuclear Island safety-related concrete.
AF-UKEPR-FS-116	The future licensee shall perform thermal analysis to confirm that the C&I and electrical equipment needed to operate the severe accident mitigation measures will remain available despite the complete loss of all HVAC systems following the severe accident sequence associated with station blackout occurring together with subsequent failure of the UDGs to start. Adequate validation evidence will need to be presented to support the thermal analysis possibly including representative testing.	Nuclear Island safety-related concrete.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-05 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-117	The future licensee shall update the PCSR to capture the revised safety case for loss of essential support systems.	Fuel to Site
AF-UKEPR-FS-118	The future licensee shall confirm that the technical specifications for control of availability of the CHRS will not allow planned maintenance to be performed on both trains of the CHRS at the same time.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-119	The future licensee shall confirm that the technical specifications for control of availability of the UDGs will not allow planned maintenance to be performed on both sets of UDGs at the same time.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-120	The future licensee shall provide a safety analysis bounding limit (SABL) for fission gas pressure distribution as a function of burn-up for incorporation into the technical specifications.	Fuel to Site

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 3

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 (GI-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.		