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-02 Revision 0 – Diversity for Frequent Faults

Assessment Report: ONR-GDA-AR-12-011
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-02** 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, EDF and AREVA were requested to demonstrate that adequate functional diversity is provided for each safety function for all frequent design basis faults. While EDF and AREVA were able to provide the required demonstration for many faults, nine areas were identified where additional information or plant modifications were required. For this reason, **GI-UKEPR-FS-02** and its associated nine actions were raised requiring EDF and AREVA to provide such demonstrations and to incorporate them within the Pre-Construction Safety Report (PCSR).

In response to GDA Issue **GI-UKEPR-FS-02**, EDF and AREVA have produced new safety submissions for each of the nine actions in order to complete the demonstration of functional diversity for frequent faults. In some cases this has resulted in design changes to the UK EPR™ protection system.

My assessment has focused on:

- The adequacy of the demonstration of functional diversity for frequent faults for the UK EPR™.
- The transient analysis performed to support the demonstration of functional diversity for excessive increase in secondary steam flow faults and Rod Cluster Control Assembly (RCCA) misalignment faults including one or more dropped RCCAs.
- Support to ONR's Control and Instrumentation (C&I) specialist inspectors in their related assessment of the functional diversity of sensors and actuators associated with the reactor protection systems under **GI-UKEPR-CI-06** and the Non-Computer based Safety System (NCSS) under **GI-UKEPR-CI-01**.
- Support to ONR's project inspector in the related cross-cutting assessment of the safety categorisation and classification of the UK EPR™ under **GI-UKEPR-CC-01**.

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 thirty-six Assessment Findings to be carried forward to the site specific detailed design phase. 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-02** (and the related GDA issues under **GI-UKEPR-CC-01**, **GI-UKEPR-CI-01** and **GI-UKEPR-CI-06**) to improve the demonstration of functional diversity for frequent faults identified in my GDA Step 4 assessment report.

The analytical work performed by EDF and AREVA has been aided by a number of important design changes to the Control and Instrumentation (C&I) systems on the UK EPR™ that in my

opinion will significantly improve the safety of the design. These changes have been proactively identified by EDF and AREVA. The changes identified are:

- Addition of a high hot leg pressure trip signal on the Safety Automation System (SAS) to improve the protection against loss of normal feedwater faults occurring together with a failure of the main reactor protection system.
- Addition of a low Reactor Coolant Pump (RCP) speed trip signal on the SAS to improve the protection against reduction in flow faults occurring together with a failure of the main reactor protection system.
- Addition of a high neutron flux trip signal and a high axial offset trip signal on the SAS to improve the protection against reactivity faults occurring together with a failure of the main reactor protection system.
- Implementation of a diverse protection function to mitigate homogeneous boron dilution faults in shutdown conditions occurring together with a failure of the main reactor protection system. The options identified for further study include provision of a diverse source range detector on the SAS or provision of a diverse boron meter on the SAS to be located on either a Nuclear Sampling System (NSS) line or the Chemical Volume and Control System (CVCS) charging or letdown line together with associated automatic protection actions.
- Upgrade to Class 2 of the actuation signal used for manually starting the Ultimate Diesel Generators (UDG).
- Upgrade to Class 2 of the actuation signal used for manually opening the Primary Depressurisation System (PDS).
- Upgrade to Class 2 of the actuation signal used for automatically closing the diverse full load Main Feedwater Isolation Valves.
- Upgrade to Class 2 of the Anticipated Trip without Scram (ATWS) signal used for the automatic actuation of the Emergency Boration System (EBS).
- Upgrade to Class 2 of the automatic CVCS charging pump switchover.
- Upgrade to Class 2 of the automatic diverse CVCS anti-dilution isolation.
- Upgrade to Class 2 of the manual start-up of the diverse third Fuel Pool Cooling System (FPCS) train.
- Upgrade to Class 2 of the FPCS purification pump trip.

Although there are a large number of Assessment Findings, these are mostly associated with the C&I protection systems. In my judgement, it is unlikely that any design changes identified as a result of the closure of these Assessment Findings will result in significant changes to plant layout.

Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that the demonstration of functional diversity for frequent faults on the UK EPR™ presented in the supporting documentation submitted in response to GDA Issue **GI-UKEPR-FS-02** is adequate 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-02** can now be closed.

LIST OF ABBREVIATIONS

ALARP	As low as is reasonably practicable
ATWS	Anticipated Transient Without Scram (Reactor Trip)
BSO	Basic Safety Objective
C&I	Control and Instrumentation
CCWS	Component Cooling Water System
CMF	Change Modification Form
CVCS	Chemical Volume and Control System
DNB	Departure from Nucleate Boiling
DSRC	Design Safety Review Committee
EBS	Emergency Boration System
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EDG	Emergency Diesel Generators
EFWS	Emergency Feedwater System
FC	Framatome Correlation
FPCS	Fuel Pool Cooling System
GDA	Generic Design Assessment
HLPD	High Linear Power Density
HSE	Health and Safety Executive
HVAC	Heating, Ventilation, and Air Conditioning
INSA	Independent Nuclear Safety Assessment
IRWST	In-containment Refuelling Water Storage Tank
LCO	Limit and Condition of safe Operation
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
MHSI	Medium Head Safety Injection
MOX	Mixed Oxide Fuel
MSRIV	Main Steam Relief Isolation Valve
MSRT	Main Steam Relief Train
MSSV	Main Steam Safety Valve
NCSS	Non-Computer based Safety System
NR	Narrow Range
NSS	Nuclear Sampling System

LIST OF ABBREVIATIONS

ONR	Office for Nuclear Regulation (an agency of HSE)
PACS	Priority Actuation Control System
PAS	Process Automation System
PCC	Plant Condition Category
PCSR	Pre-construction Safety Report
PDS	Primary Depressurisation System
POSR	Pre-operational Safety Report
PS	Protection System
PSA	Probabilistic Safety Analysis
PSV	Pressuriser Safety Valve
PWR	Pressurised Water Reactor
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHRS	Residual Heat Removal System
RRC	Risk Reduction Category
SAP	Safety Assessment Principle(s) (HSE)
SAS	Safety Automation System
SBLOCA	Small Break Loss of Coolant Accident
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIS	Safety Injection System
SLB	Steam Line Break
SSS	Start-Standby System
SPND	Self-Powered Neutron Detector
TAG	Technical Assessment Guide(s) (ONR)
TQ	Technical Query
TXS	C&I Digital Computer Platform
WR	Wide Range
UDG	Ultimate Diesel Generator
URBWP	Uncontrolled RCCA Bank Withdrawal at Power

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 a number of GDA Issues and 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 to the site specific detailed design phase.

4 During the GDA assessment EDF and AREVA were asked to demonstrate that adequate functional diversity is provided for each safety function for all frequent design basis faults. While EDF and AREVA were able to provide the required demonstration for many faults, nine areas were identified where additional information or plant modifications were required. For this reason, **GI-UKEPR-FS-02** was raised requiring EDF and AREVA to provide such demonstrations and to incorporate them within the Pre-Construction Safety Report (PCSR).

5 The aim of this assessment is to provide a comprehensive assessment of the submissions provided in response to GDA Issue **GI-UKEPR-FS-02** 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. The 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-02** (Ref. 1), this assessment focuses on:

- The adequacy of the demonstration of functional diversity for frequent faults for the UK EPR™ using functional analysis.

- The transient analysis performed to support the demonstration of functional diversity for excessive increase in secondary steam flow faults and Rod Cluster Control Assembly (RCCA) misalignment faults including one or more dropped RCCAs.
- Support to ONR's C&I specialist inspectors in their related assessment of the functional diversity of sensors and actuators associated with the reactor protection systems under **GI-UKEPR-CI-06** and the non-computer based safety systems (NCSS) under **GI-UKEPR-CI-01**.
- Support to ONR's project inspector in the related cross-cutting assessment of the safety categorisation and classification of the UK EPR™ under **GI-UKEPR-CC-01**.

8 The purpose of this assessment is to consider whether the deliverables provided in response to the GDA Issue, **GI-UKEPR-FS-02**, and the associated nine GDA Issue Actions, provide an adequate response sufficient to justify closure of the issue. The GDA Issue together with the nine actions 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™ (Ref. 2) in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process.

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 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 demonstration of functional diversity for frequent 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 DIVERSITY FOR FREQUENT FAULTS

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), identified 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-02** 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 demonstration of functional diversity for frequent faults.
- 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 Modification Form (CMF).
- In addition to, and as result of, the assessment of the submissions made in accordance with the resolution plan, a number of Technical Queries (TQs) were issued. The responses made by EDF and AREVA to the TQs (Ref. 9) have 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 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 GDA close-out phase for this issue and other related issues and so assessment work has been co-ordinated with the C&I topic lead on sensor and actuator diversity (Refs 10 & 11), the Probabilistic Safety Analysis (PSA) topic lead on NCSS functionality (Ref. 12) and with the Human Factor (Ref. 13) topic lead on station blackout sequences.

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. Of these, those that are relevant to functional diversity for frequent faults are the control and limitation functions within the reactor control, surveillance and limitation (RCSL) system, the development of suitable Operational Technical Specifications and operation with mixed oxide fuel (MOX) in the reactor.

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 into the component GDA Issue Actions and then further broken down into specific deliverables for detailed assessment:

GDA Issue Action	Technical Area	Deliverable	Ref.
GI-UKEPR-FS-02.A1	Loss of normal feedwater faults	Change Modification Form #23	8
GI-UKEPR-FS-02.A2	Excessive increase in steam flow faults	PEPR-F DC 84 Rev A	14
GI-UKEPR-FS-02.A3	Reduction in RCS flow faults	Change Modification Form#23	8
GI-UKEPR-FS-02.A4	Uncontrolled RCCA bank withdrawal faults	Change Modification Form#23	8
GI-UKEPR-FS-02.A5	RCCA misplacement faults	PEPCF.11.1467 Rev 0	15
GI-UKEPR-FS-02.A6	Loss of CVCS faults	PEPR-F 11.0956 Rev 1	16
GI-UKEPR-FS-02.A7	Homogeneous boron dilution faults	PEPCF.12.0678 Rev 1	17
GI-UKEPR-FS-02.A7	Homogeneous boron dilution faults	Change Modification Form#59	8
GI-UKEPR-FS-02.A8 and A9	Loss of support system faults	Letter EPR01281N	18
GI-UKEPR-FS-02.A8	Loss of support system faults	ECESN120274 Rev A	19
GI-UKEPR-FS-02.A8	Loss of support system faults	Letter EPR01386N	20
GI-UKEPR-FS-02.A9	Diverse safe shutdown state	NEPR-F DC 580 Rev B (included in full as update to PCSR Chapter 16.5)	21
GI-UKEPR-FS-02.A1 to A9	PCSR – Chapter 14.7 PCSR – Chapter 16.5	Fault and Protection Schedule Adequacy of the UK EPR design regarding functional diversity	21

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. 22) which has already been subject to assessment during earlier stages of GDA. In addition, it is important to note that the deliverables are not intended to provide the complete safety case covering functional diversity for frequent faults. Rather they form further detailed arguments and evidence to supplement those already provided during earlier steps within the GDA Process.

Change Modification Form #23: Additional reactor trips on SAS C&I system

24 The purpose of Change Modification Form (CMF) #23 (Ref. 8) is to outline the proposed modification identifying the additional reactor trip signals to be provided on the SAS to ensure adequate functional diversity. It is proposed to add four additional reactor trip signals, high hot leg pressure, low RCP speed, high neutron flux and high axial offset, to the SAS to provide diverse protection against loss of normal feedwater faults, reduction in Reactor Cooling System (RCS) coolant flow faults, and uncontrolled RCCA bank withdrawal at power faults. Stage 1 of the modification giving a description and rationale for the change was submitted during Step 4 in January 2011. In order to complete the six-step design change procedure agreed for GDA it was necessary for EDF and AREVA to also complete Stage 2 of the modification by performing an impact analysis on the GDA submission documentation and Stage 3 of the modification by providing a handover package for a future licensee. In response to Actions 1, 3 & 4 of **GI-UKEPR-FS-02**, EDF and AREVA have therefore updated CMF#23 (Ref. 8).

Excessive increase in steam flow – Sensitivity Analyses

25 This report (Ref. 14) presents the results of transient analysis sensitivity studies performed with the aim of demonstrating that adequate diverse protection is already provided on the UK EPR™ to protect against an excessive increase in secondary steam flow fault occurring while the reactor is at full power. The report has been produced in response to Action 2 of GDA issue **GI-UKEPR-FS-02**.

Anticipated Transient Without Scram (ATWS) by loss of TXS – RCCA misalignment fault (up to one or more dropped RCCA)

26 This report (Ref. 15) presents the results of transient analysis studies performed with the aim of demonstrating that adequate diverse protection is already provided on the UK EPR™ to protect against a RCCA misalignment fault up to one or more dropped RCCAs. The report has been produced in response to Action 5 of GDA issue **GI-UKEPR-FS-02**.

Diverse protection against loss of CVCS following reactor trip

27 This report (Ref. 16) demonstrates the provision of diverse protection against the loss of the Chemical Volume Control System (CVCS) following reactor trip and the associated xenon decay including a demonstration of diversity to operator action. The report has been produced in response to Action 6 of GDA issue **GI-UKEPR-FS-02**.

Development of a diverse protection system for CVCS homogeneous boron dilution events in shutdown states

28 The purpose of this report (Ref. 17) is to present an As low as is reasonably practicable (ALARP) assessment to identify a means of providing diverse protection against frequent homogeneous boron dilution faults occurring during shutdown conditions in coincidence with the common mode failure of the main reactor Protection System (PS). The report identifies the need to add an additional sensor to the Safety Automation System (SAS) to provide diverse protection against such faults. The report has been produced in response to Action 7 of GDA issue **GI-UKEPR-FS-02**.

CMF#59: Diverse protection function for CVCS homogeneous boron dilution events in shutdown states

29 The purpose of CMF#59 (Ref. 8) is to propose the modification identified in the previous report (Ref. 17), which is to add an additional sensor to the SAS to provide diverse protection against CVCS faults resulting in homogeneous boron dilution faults during shutdown operations. CMF#59 (Ref. 8) has also been produced in response to Action 7 of GDA Issue **GI-UKEPR-FS-02**.

Diversity for frequent faults – Loss of support systems

30 The purpose of this letter (Ref. 18) 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 Component Cooling Water System (CCWS), loss of one division of the safeguard building Heating, Ventilation, and Air Conditioning (HVAC) system, or one division of the safeguard building essential electrical system. The letter has been produced in response to Actions 8 and 9 of GDA issue **GI-UKEPR-FS-02**.

Diversity for Frequent Faults – ATWS LOOP cumulated with automatic EDG start-up failure

31 This report (Ref. 19) presents an ALARP assessment into the feasibility of providing an automatic means of starting up the Ultimate Diesel Generators (UDGs) following a Loss of Off-site Power (LOOP) fault in coincidence with failure of the PS to automatically start the Emergency Diesel Generators (EDGs). The report has also been produced in response to Action 8 of GDA issue **GI-UKEPR-FS-02**.

Diverse protection for the frequent faults involving the loss of essential support systems – Loss of off-site power with station blackout event

32 This report (Ref. 20) provides further justification of the protection provided for the fault sequence involving a LOOP fault in coincidence with failure of the PS to automatically start the Emergency Diesel Generators (EDGs). The report has also been produced in response to Action 8 of GDA issue **GI-UKEPR-FS-02**.

Functional diversity for frequent faults

33 The aim of this report which has been fully incorporated into Sub-Chapter 16.5 of the PCSR (Ref. 21) is to demonstrate that for each frequent design basis fault a diverse means of achieving each safety function is available for reaching the safe shutdown state from the controlled state. The report has been produced in response to Action 9 of GDA issue **GI-UKEPR-FS-02**.

PCSR Updates

34 In addition to the technical reports, EDF and AREVA have also provided updates (Ref. 21) to the March 2011 PCSR (Ref. 23) for Chapter 14.7 on the fault and protection schedule and Chapter 16.5 on function diversity for frequent faults.

4 ONR ASSESSMENT

35 My assessment against the SAPs of the UK EPR™ safety submissions covering the demonstration of functional diversity for frequent faults is presented below.

36 Sections 4.1 to 4.9 present the assessments of the responses to the nine actions associated with GDA Issue **GI-UKEPR-FS-02**. The first five actions (Sections 4.1 to 4.5) are associated with the provision of diverse reactor trip signals on the SAS for loss of normal feedwater faults, excessive increase in secondary steam flow, reduction in RCS flow, uncontrolled RCCA bank withdrawal at power faults, and RCCA misplacement faults. Actions six and seven (Sections 4.6 and 4.7) are associated with the provision of diverse reactivity control on a shutdown reactor. Specifically, Action 6 covers reactor trip with loss of the CVCS while Action 7 covers homogeneous boron dilution faults during shutdown conditions. Action 8 (Section 4.8) is associated with the provision of diverse protection following loss of essential support systems while Action 9 (Section 4.9) is associated with the provision of diverse protection to reach the safe shutdown state.

37 Section 4.10 reviews the minutes of the 10th UK EPR™ Design Safety Review Committee which included an independent peer review of PCSR Chapter 16.5 on functional diversity for frequent faults. Section 4.11 provides a brief review of the updates to those areas of the PCSR concerning the demonstration of functional diversity for frequent faults.

38 Sections 4.12, 4.13 and 4.14 provide cross-cutting supporting assessments of related technical areas associated with the demonstration of functional diversity. This includes the assessment of C&I sensor and actuator diversity and the functional scope of the NCSS as well as reviewing the classification of the CVCS given its potential role as a diverse means of safety injection on the UK EPR™.

39 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 to the site specific detailed design phase. These are listed in Annex 2.

4.1 Diverse Protection for Loss of Normal Feedwater Faults (Action 1)

4.1.1 Summary of EDF and AREVA's Safety Case

40 This fault sequence involves the loss of normal feedwater flow coincident with the common mode failure of the PS. During Step 4 of GDA, EDF and AREVA identified the need for an additional automatic reactor trip signal based upon detection of high hot leg pressure to be implemented on the SAS in addition to a claim on the automatic actuation signal for the Emergency Feedwater System (EFWS) based upon detection of low Steam Generator (SG) level to be implemented on the NCSS (see Section 4.14.2 below) to provide diverse protection against this fault. Stage 1 of CMF#23 (Ref. 8) was therefore raised proposing the design change to the SAS. EDF and AREVA argue that when the design change is implemented adequate protection will be provided against the fault.

4.1.2 Assessment

41 The proposed modification to provide an additional automatic reactor trip signal based upon detection of high hot leg pressure on the SAS was assessed by ONR in the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2). This assessment concluded that the proposed modification was a major safety improvement, the implementation of which was fully supported. However, there was need to complete the six-stage design change

procedure for GDA (Ref. 24) by providing Stages 2 and 3 of CMF#23 (Ref. 8). For this reason, Action 1 of GDA issue **GI-UKEPR-FS-02** was raised to close out the modification for the purposes of GDA.

42 In response to Action 1 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have provided Stages 2 and 3 of CMF#23 (Ref. 8). Stage 2 of the CMF provides an impact analysis on the GDA submission documentation while Stage 3 provides a handover package for a future licensee. I have reviewed the submissions and I am content that the updates provide an adequate record of the proposed design change to handover to a future licensee so as to enable full implementation of the design change during the site specific detailed design phase. ONR will be able to monitor the completion of this modification through the generic cross-cutting Assessment Finding **AF-UKEPR-CC-01**. For this reason, in my opinion, Action 1 of GDA issue **GI-UKEPR-FS-02** can now be closed.

4.1.3 Findings

43 Following my assessment of the EDF and AREVA submission, I am content for Action 1 of GDA Issue **GI-UKEPR-FS-02** to be closed. I have no additional assessment findings.

4.2 Diverse Protection for Excessive Increases in Secondary Steam Flow (Action 2)

4.2.1 Summary of EDF and AREVA's Safety Case

44 This fault sequence involves an excessive increase in secondary steam flow due to either the spurious opening of a Main Steam Relief Train (MSRT) or Main Steam Safety Valve (MSSV), or the Main Steam Bypass (MSB) system or a steam system piping failure together with failure of the reactor to trip due to either mechanical failure of the RCCAs to insert or failure of the protection system to generate a reactor trip signal. Such faults result in an increase in the reactivity and power of the core potentially threatening the integrity of the fuel cladding should a departure from nucleate boiling (DNB) occur.

45 The basis of the EDF and AREVA safety case is that they have performed transient analysis studies of the sequence including sensitivities to the initial axial offset and moderator temperature coefficients and demonstrated that significant fuel damage will not occur. EDF and AREVA conclude that on the basis of the transient analysis presented adequate protection is provided against this fault.

4.2.2 Assessment

46 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2), I provided an assessment of the EDF and AREVA transient analysis studies for the sequences excessive increase in secondary steam flow with mechanical failure of the RCCAs to insert and excessive increase in secondary steam flow with failure of the protection system to trip the reactor.

47 In my assessment (Ref. 2), I noted that in the case of excessive increase in steam flow with failure of RCCAs to insert the fault is seen to cause a corresponding increase in reactor power from 100% to 115%. The minimum DNBR is claimed to remain above 1.0

although no plot is presented of the parameter[1]. In a later (TQ) response (TQ-EPR-1432, Ref. 9) EDF and AREVA claim to show that the DNBR remains greater than 1.9 when calculated using the MANTA, SMART, and FLICA III coupled codes but the timings on the transient look inconsistent to those of the earlier transient. In the initial analysis provided (Ref. 23) beginning of cycle conditions with a moderator coefficient of -13.2 pcm/°C and an initial boron concentration of 1594 ppm are assumed, which are claimed to be bounding on the grounds they minimises the power reduction once the RCPs are tripped. Given that the initiating event is a cooldown transient, my concern is more with the initial reduction in the minimum DNBR and so it is not obvious that these assumptions are bounding. Furthermore, the minimum DNBR occurs before the time when normal reactor trip would occur anyway and so this is an issue associated with the effectiveness of 1st line tripping and not the low frequency ATWS sequence. The reactor trip signal occurs on low SG level after 313 seconds and turbine trip follows shortly afterwards causing reactor power to decrease. The ATWS signal occurs at 333 seconds following failure of the RCCAs to insert, causing the Emergency Boration System (EBS) to inject borated water. The RCPs are tripped after 397 seconds on low SG level.

48 My assessment (Ref. 2) also noted, as with the ATWS case with mechanically stuck RCCAs, that the excessive increase in steam flow with failure of the protection system case causes the reactor power to increase from 100% to 115% and the minimum DNBR decreases to a value of 1.1. The analysis again assumes beginning of cycle conditions. However, the failure of the RPS means that the reactor can only be tripped on the diverse protection system which results in a significant delay in the trip which does not occur until 923 seconds.

49 Finally, my assessment (Ref. 2) also noted that these same faults are also studied in the RRC-A analysis in Chapter 16.1 of the PCSR (Ref. 23). It is noticeable that the transient studies performed in the functional diversity review are significantly worst than the ones reported in the RRC-A analysis. These differences are judged to be more than can be explained by the application of best estimate assumptions made in the RRC-A analysis. From discussions with EDF and AREVA it is apparent that the design change associated with increasing the cooldown rate in response to small break loss of coolant accidents from 100°C/hr to 250°C/hr has resulted in a relaxation of the SG pressure drop trip set point which now means that the low SG level is the most effective trip parameter for these faults.

50 On the basis of my GDA Step 4 assessment, Action 2 of GDA issue **GI-UKEPR-FS-02** was raised for EDF and AREVA to perform an ALARP review into feasibility of providing an additional diverse trip signal or tightening the existing protection set points for this fault.

51 In response to Action 2 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed (Ref. 14) some additional sensitivity studies for the two ATWS sequences in which they have varied axial offset, moderator feedback coefficient and the assumed steam flow rate. The results show very little sensitivity to changes in these parameters.

52 In the case of mechanical failure of the RCCAs to insert the minimum DNBR is 1.01. For beginning of cycle conditions, changes in axial offset ranging from +12% to -30% only reduce the minimum DNBR to 0.99. Even for end of cycle conditions, the same changes

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

in axial offset result in a minimum DNBR of 0.97. Similarly, in the case of the protection system failure the minimum DNBR is 1.03. For beginning of cycle conditions this reduces to 1.00 for the sensitivity to axial offset. For end of cycle conditions this reduces to 0.97. I was slightly surprised by these results as I would have expected the DNBR value to be very sensitive to axial offset and so I raised TQ-EPR-1593 for further clarification. In their response, EDF and AREVA explain (Ref. 9) that they have not performed coupled 3D calculations for these transients. Hence, the sensitivity studies to axial offset only effect the thermal hydraulic system calculations and not the fuel performance calculations that determine the fuel DNBR. In the latter calculations, the value of the radial power distribution factor, $F_{\Delta H}$, is set to 2.09 and the axial offset is put to 1.0. Since, the peak $F_{\Delta H}$ will be limited to the design value of 1.5 in practice this will accommodate a peak axial offset of approximately 1.9 given that deposition controlled dryout scales roughly as $F_{\Delta H}^2$. The initial value of $F_{\Delta H}$ is therefore very conservative and is selected to match the Limit and Condition of safe Operation (LCO) limit for DNBR of 1.32. The fact that these parameters were kept constant throughout all the sensitivity studies explains the apparently limited impact of the variations in axial offset.

53 Significantly, the analysis report (Ref. 14) notes that the calculations do not model the $DNBR_{low}$ trip despite the fact that this can provide an automatic first line trip given that the transient is sufficiently slow to allow the in-core detectors to be effective. This is major conservatism in the analysis that I was not aware of when assessing the original calculations during Step 4 of GDA (Ref. 2) and removes my concerns about first line tripping.

54 The analysis report (Ref. 14) also presents a sensitivity study on steam flow rates corresponding to 108% and 118% flow where the latter corresponds to the base case flow. Not surprisingly, the reduction in flow improves the minimum DNBR to 1.10 and 1.11 for the mechanical and protection system failure ATWS cases respectively. The 118% case corresponds to the opening of a single valve on the bypass system. It should be noted that the MSSV and MSRT valves have a much greater flow capacities, an MSRT valve being able to pass approximately 50% of the capacity of a main steamline. The possibility of a spurious C&I signal causing multiple valve openings also has to be considered. For this reason, TQ-EPR-1593 (Ref. 9) also requested EDF and AREVA to perform a parametric study of all the different trip parameters (low SG level, high core power, low SG pressure, $DNBR_{low}$ and SG pressure drop) as a function of flow (or equivalent break area) up to the spurious lifting of all four MSRTs. In response, EDF and AREVA have performed some further transient analysis studies (Ref. 24). The results are presented in a table which presents for each trip parameter, the time in a transient when the trip parameter is reached (for those cases were it is effective) as a function of equivalent break size from 200 cm^2 to 2000 cm^2.

55 The analysis clearly demonstrates that the $DNBR_{low}$ trip parameter is effective for all break sizes. It also demonstrates that the SG pressure drop signal is also an effective trip parameter for break sizes greater than 1000 cm^2 confirming that there is always a first line trip parameter that will avoid DNB. Furthermore, in addition to demonstrating that there is an effective first line trip, it also demonstrates that the ATWS case associated with mechanical failure of the RCCAs to insert is also effectively protected against. This is because the $DNBR_{low}$ trip will be a faster acting trip than the low SG level trip currently claimed in Chapter 16.5 of the PCSR analysis (Ref. 23). Once a reactor trip signal is generated it will actuate the ATWS signal which automatically trips the RCPs and actuates the EBS rapidly reducing core power and protecting against DNB.

56 By extrapolating from the results in the table (Ref. 24) it is possible to judge that for break sizes greater than 2000 cm^2 the low SG pressure signal is also likely to be an effective trip parameter. Likewise, for break sizes less than 200 cm^2 it can be deduced that the reactor will reach a new steady state condition with a slightly higher reactor power for which DNB will not occur. However, in the range 200 cm^2 to 1000 cm^2, which includes the range of most interest for spurious MSRT opening, the $DNBR_{low}$ trip is the only effective trip parameter. EDF and AREVA argue that the high core power level trip would be effective over much of this range if some of the conservatism in the analysis were to be removed. However, the high core power trip, like the $DNBR_{low}$ trip, is a trip parameter that is only available on the PS. It does not provide a signal to the SAS/NCSS C&I safety systems and so no diversity is demonstrated for the excessive increase in steam flow ATWS case with failure of the PS. In particular, EDF and AREVA acknowledge that the claim on low SG level trip currently presented in Chapter 16.5 of the PCSR (Ref. 23) cannot be sustained because of uncertainty in how the fault will interact with the SG level controller. Instead, they have conservatively modelled the feedwater flow as matching the steam flow since this maximises the cooldown capability of the affected SG.

57 In response to this shortcoming, EDF and AREVA (Ref. 14) make the judgement that the high neutron flux signal provided on the SAS/NCSS will provide an effective trip parameter over the range of break sizes required. However, they are not currently able to model the ex-core detectors using the MANTA computer code and so are unable to fully substantiate this judgement. To overcome this problem, it will be necessary to incorporate a representation of the ex-core detectors into the code using importance data derived from detector transport models. Nevertheless, I recognised that ex-core detectors have traditionally been used as the primary flux protection system on PWRs. Although the UK EPR™ has a heavy reflector, this is unlikely to prevent the detectors from performing this function at full power. A further issue might be the slight reduction in the temperature of the water in the RPV downcomer as a result of the cooldown fault such that use of the ex-core flux detectors is a potential problem. However, if this is a problem, there is the possibility of altering the processing logic for the detectors. For these reasons, I tend to share the judgement of EDF and AREVA that the ex-core detectors will provide effective protection for this fault. Nevertheless, I have raised Assessment Finding **AF-UKEPR-FS-41** for a future licensee to confirm the effectiveness of the high flux trip signal generated on the ex-core detectors as diverse means of protection for excessive increase in secondary steam flow faults.

58 In summary, I accept that there is a first line of protection that will avoid DNB over the full range of excessive increase in secondary steam flow faults. I also accept that the $DNBR_{low}$ trip will provide an effective signal to protect against the ATWS case of mechanical failure of the RCCAs to insert meeting the requirements of SAP FA.7. My judgement is that the ex-core flux detectors will also provide effective protection against the ATWS case of failure of the PS to trip the reactor and that this might be possible without the need for any design changes. However, further work will be required to fully substantiate this claim and so I have raised Assessment Finding **AF-UKEPR-FS-41** for a future licensee to perform this work. Nevertheless, on the basis of the evidence provided, I am satisfied that sufficient progress has been made to justify closure of Action 2 of GDA Issue **GI-UKEPR-FS-02**.

4.2.3 Findings

59 Following my assessment of the EDF and AREVA submission, I am content for Action 2 of GDA issue **GI-UKEPR-FS-02** to be closed. Assessment Finding **AF-UKEPR-FS-41** has been raised for a future licensee to demonstrate that the ex-core detectors provide a

diverse means of protection against the excessive increase in secondary steam flow faults.

4.3 Diverse Protection for Reduction in RCS Flow Faults (Action 3)

4.3.1 Summary of EDF and AREVA's Safety Case

60 This fault sequence involves a reduction in RCS flow in coincidence with the common mode failure of the PS. During Step 4 of GDA, EDF and AREVA identified the need for an additional automatic reactor trip signal based upon detection of low RCP speed to be implemented on the SAS to provide diverse protection against this fault. Stage 1 of CMF#23 (Ref. 8) was therefore raised proposing the design change. EDF and AREVA argue that with the design change implemented adequate protection is provided against this fault.

4.3.2 Assessment

61 The proposed modification to provide an additional automatic reactor trip signal based upon detection of low RCP speed on the SAS was assessed by ONR in the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2). This assessment concluded that the proposed modification was a positive development from a safety perspective and that its implementation was fully supported. However, there was a need to complete the six stage design change procedure for GDA (Ref. 24) by providing Stages 2 and 3 of CMF#23 (Ref. 8). For this reason, Action 3 of GDA issue **GI-UKEPR-FS-02** was raised to close out the modification for the purposes of GDA.

62 In response to Action 3 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have provided Stages 2 and 3 of CMF#23. Stage 2 of the CMF provides an impact analysis on the GDA submission documentation while Stage 3 provides a handover package for a future licensee. I have reviewed the submission and I am content that the updates provide an adequate record of the proposed design change to handover to a future licensee to enable full implementation of the design change during the site specific detailed design phase. ONR will be able to monitor the completion of this modification through the generic cross-cutting Assessment Finding **AF-UKEPR-CC-01**. For this reason, in my opinion, Action 3 of GDA issue **GI-UKEPR-FS-02** can now be closed.

4.3.3 Findings

63 Following my assessment of the EDF and AREVA submission, I am content for Action 3 of GDA Issue **GI-UKEPR-FS-02** to be closed. I have no additional assessment findings.

4.4 Diverse Protection for Uncontrolled RCCA Bank Withdrawal Faults (Action 4)

4.4.1 Summary of EDF and AREVA's Safety Case

64 This fault sequence involves the uncontrolled withdrawal of an RCCA bank with the reactor at power coincident with the common mode failure of the PS. During Step 4 of GDA, EDF and AREVA identified the need for additional automatic reactor trip signals based upon detection of high neutron flux and high axial offset to be implemented on the SAS to provide diverse protection against this fault. Stage 1 of CMF#23 (Ref. 8) was therefore raised proposing the design change. EDF and AREVA argue that with the design change implemented adequate protection is provided against this fault.

4.4.2 Assessment

65 The proposed modification to provide two additional automatic reactor trip signals based upon detection of high neutron flux and high axial offset on the SAS was assessed by ONR in the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2). This assessment concluded that the proposed modification represented a significant safety improvement and that its implementation was fully supported. However, there was need to complete the six stage design change procedure for GDA (Ref. 24) by providing Stages 2 and 3 of CMF#23. For this reason, Action 4 of GDA issue **GI-UKEPR-FS-02** was raised to close out the modification for the purposes of GDA.

66 In response to Action 4 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have provided Stages 2 and 3 of CMF#23. Stage 2 of the CMF provides an impact analysis on the GDA submission documentation while Stage 3 provides a handover package for a future licensee. I have reviewed the submission and I am content that the updates provide an adequate record of the proposed design change to handover to a future licensee to enable the full implementation of the design change during the site specific detailed design phase. ONR will be able to monitor the completion of this modification through the generic cross-cutting Assessment Finding **AF-UKEPR-CC-01**. It should also be noted that this generic cross cutting Assessment Finding is reinforced by the pre-existing Assessment Finding **AF-UKEPR-FS-15** requiring a future licensee to perform additional transient analysis to demonstrate that for the uncontrolled RCCA bank withdrawal fault at power there is a diverse trip signal available for the full range of reactivity insertion rates and power levels. For these reasons, in my opinion, Action 4 of GDA issue **GI-UKEPR-FS-02** can now be closed.

4.4.3 Findings

67 Following my assessment of the EDF and AREVA submission, I am content for Action 4 of GDA Issue **GI-UKEPR-FS-02** to be closed. I have no additional assessment findings.

4.5 Diverse Protection against RCCA Misplacement Faults (Action 5)

4.5.1 Summary of EDF and AREVA's Safety Case

68 This fault sequence involves an RCCA misplacement fault (including up to one or more dropped RCCAs) occurring together with the failure of the protection system to generate a reactor trip. RCCA misalignment faults results in a localised asymmetric distortion of the flux distribution resulting in the fuel generating power in localised areas in excess of the cooling provisions. In particular, in the case of dropped RCCA faults, the initial drop in core power caused by the initiating fault results in the relative up rating of those regions of the core remote from the fault due to the effects of the reactor control system, the moderator feedback effects associated with the initial cooldown, and changes in the xenon distribution.

69 The basis of the EDF and AREVA safety case is that they have reviewed what they regard as the most of onerous of the frequent faults (the drop of 3-out-of-4 RCCAs associated with a single control group resulting in single RCCAs dropping in 3 of the 4 quadrants of the core). For this case they have performed detailed transient analysis studies and demonstrated that providing the reactor is sufficiently well trimmed prior to the fault occurring it is able to ride out the transient without significant fuel damage occurring.

70 EDF and AREVA argue that on the basis of the transient analysis presented adequate protection is provided for the full range of faults considered.

4.5.2 Assessment

71 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2), it was noted that no analysis of this fault with failure of the protection system or the in-core detector system to trip was provided in the review of functional diversity. For this reason, Action 5 of GDA issue **GI-UKEPR-FS-02** was raised for EDF and AREVA to provide such analysis.

72 In response to the Action 5 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed transient analysis studies (Ref. 15) to demonstrate that providing the reactor is well trimmed prior to the fault occurring based upon measurements made using the in-core Self-Powered Neutron Detectors (SPND) to demonstrate compliance with the limits on conditions for safe operation such as $DNBR_{SAL}$[1] then the reactor can ride out the transient without significant fuel damage or the need for a diverse reactor trip signal. To better understand the approach being adopted TQ-EPR-1581 (Ref. 9) was raised for EDF and AREVA to provide further clarification on the calculations performed.

73 The methodology can be explained as follows. A series of decoupled calculations are performed in three stages. The first stage involves performing numerous static 3D reactor physics calculations to identify those RCCA drop cases that result in the greatest up-rating in the radial power factor, $F_{\Delta H}$, which is given the symbol $\Delta F_{\Delta H}$. For a given maximum value of $\Delta F_{\Delta H}$ a search for the minimum RCCA worth needed to achieve this change is made, since for a constant load demand this minimises the neutronic feedback in relation to the power increase. Beginning of cycle conditions are also used. Although these fuel cycle conditions increase the temperature reduction during the transient for a given RCCA worth compared with end of cycle conditions the early cycle conditions have been found to result in more bounding values for $\Delta F_{\Delta H}$ which is the dominant parameter driving this fault. The calculations performed are not for the UK EPR™ design since an appropriate MANTA input deck is not currently available. EDF and AREVA judge that this will have minimal impact on the results although this will need to be confirmed by a future licensee during the site specific detailed design phase in line with the requirements of pre-existing Assessment Finding **AF-UKEPR-FS-08** which requires that all analysis should reflect the UK EPR™ design. From the results of this analysis, the most onerous condition was found to have a $\Delta F_{\Delta H}$ of 19%. This corresponded to the case of three dropped RCCAs, each one dropping in one of three different quadrants of the core.

74 Once the most onerous RCCA drop case has been established the second stage of the analysis process is to perform a coupled 3D thermal hydraulic and reactor physics transient calculation to determine the overall system response in terms of variations in reactor power, pressure and inlet temperature to provide boundary conditions for the fuel performance calculation. The coupled MANTA and SMART codes were used to perform this analysis. These computer codes were assessed against the requirements of SAPs FA.17 to FA.19 and FA.21 to FA.22 during Step 4 of GDA (Ref. 2) where it was concluded that they were fit for purpose although a number of Assessment Findings were identified to help improve the validation evidence.

75 The final stage of the analysis process is to perform the fuel analysis to determine the conditions of the fuel during the fault. A decoupled calculation is performed in which a conservative value for axial offset of 30% is assumed together with an onerous initial

[1] $DNBR_{SAL}$ (Safety Analysis Limit) corresponds to the $DNBR_{LCO}$ (Limit and Condition for Safe Operation) threshold at site with the exception that the uncertainties associated with the critical heat flux correlation and the rod bow penalty have been removed since these are explicitly modelled within the analysis for this fault.

$\Delta F_{\Delta H}$ determined to ensure the limiting $DNBR_{SAL}$ value applies at the start of the transient. The choice of axial offset is conservative since the LCO is currently 12%. The value corresponds to the initial set point proposed by EDF and AREVA for the high axial offset trip signal on ex-core neutron flux detectors that is being provided on the SAS in response to Action 4 of GDA issue **GI-UKEPR-FS-02** discussed in Section 4.4.2 above. This is a very high value and a future licensee will need to demonstrate it is ALARP not to reduce this set point so as to avoid DNB in response to Assessment Findings **AF-UKEPR-FS-15** raised in the GDA Step 4 report (Ref. 2) and **AF-UKEPR-FS-41** raised in Section 4.2.2 above. These boundary conditions are then combined with the maximum $\Delta F_{\Delta H}$ determined from the earlier reactor physics calculations.

76 The results of the calculations are that the number of fuel rods experiencing boiling crisis remains below 1% during the transient and the maximum cladding temperature reached during the transient remains below 1190°C ensuring the structural integrity of the fuel is maintained. I accept that this is a conservative calculation meeting the requirements of SAP FA.7. It confirms, that providing the initial core parameters are compliant with the LCOs, as demonstrated using the in-core detectors, the reactor is able to ride out the transient without significant fuel damage or the need for a diverse reactor trip signal. One of my motivations for raising Action 5 of GDA issue **GI-UKEPR-FS-02** is that Sizewell B is provided with a negative rate flux trip on the ex-core detectors to specifically protect against dropped RCCA faults. It is noted that as a risk reduction measure, in certain fault situations the UK EPR™ has been designed to perform a rapid power reduction transient using the turbine limitation functions of the RCSL system on order to avoid unnecessary reactor trips. However, such transients would be likely to cause the negative flux rate trip to operate unnecessarily. Given the effectiveness of the in-core detectors in protecting against this fault and the undesirability of tripping following a turbine power reduction transient, I accept it would be disproportionate to insist on a diverse negative flux rate trip signal being provided on the UK EPR™. I am therefore content for Action 5 of GDA issue **GI-UKEPR-FS-02** to be closed.

77 Given their importance in protecting against RCCA misalignment faults an assessment of the design and function of the in-core detector system has been made and is presented in the following paragraphs. The in-core detectors are used to provide both the $DNBR_{low}$ and the High Linear Power Density (HLPD) trip signals and consist of 72 SPNDs that are located within twelve fingers at six axial locations. Each SPND finger is located in an instrumentation guide tube within a fuel assembly. The location of the twelve SPND fingers is chosen to give as good coverage as possible over the whole core. The SPNDs consist of a Cobalt-59 sensor emitter which absorbs neutrons to create Cobalt-60 and Cobalt-61 which decay producing gamma-rays and beta particles with characteristic half-lives. The beta particles generate a current in the sensor sheath that can be measured and is proportional to the local neutron flux. Given that the SPNDs are relatively simple passive devices for which there is considerable operating experience gained from their use on the German KONVOI reactor fleet, their incorporation into the UK EPR™ design represents, in my judgement, a major safety improvement on earlier generations of PWRs.

78 The HLPD trip uses the 72 SPND detectors to directly determine the maximum linear power density. The trip is generated on the second highest value found on any SPND when it exceeds a set point value. This set point value is adjusted should a detector be revealed as not working. The four C&I divisions all share the 72 SPND outputs with trip voting between the four C&I divisions done on a 2-out-of-4 basis. The detectors are periodically calibrated against a flux map generated at six axial levels using the aero-ball system and comparison with a reference heat balance.

79 The $DNBR_{low}$ trip also uses input from the 72 SPNDs together with measurements of primary pressure and inlet temperature which determine the inlet coolant density and RCP speed to determine the primary coolant flow rate. This information is then used to calculate the minimum DNBR value online. The axial profile is reconstructed for each of the twelve fingers using the six axial measurements with 12 SPNDs per axial level. The critical heat flux is calculated using these boundary values and the Framatome Correlation (FC) critical heat flux correlation that was assessed during Step 4 of GDA (Ref. 2). As with the HLPD, the trip is generated on the second highest value when it exceeds a set point value. Again, this set point value is adjusted should a detector be revealed as not working. The four C&I divisions all share the twelve DNBR outputs with trip voting between the four C&I divisions done on a 2-out-of-4 basis. Again, the detectors are periodically calibrated against the flux map generated at six axial levels using the aero-ball system and comparison with a reference heat balance.

80 In the case of asymmetric faults, such as RCCA misalignment faults, additional voting logic is applied to optimise the performance of the $DNBR_{low}$ trip. As well as the twelve on-line DNBR calculations, measurements of RCCA insertion and withdrawal rates and comparisons of symmetrical partners from the 72 SPND linear power density measurements are used to refine the tripping criteria as follows:

- Tripping on the 2nd minimum DNBR value from the twelve on-line DNBR calculations using 2-out-of-4 C&I divisional voting.
- Tripping on the 1st minimum DNBR value from the twelve on-line DNBR calculations using 2-out-of-4 C&I divisional voting when in-coincidence with a high RCCA insertion or withdrawal rate using 1-out-of-4 C&I divisional voting.
- Tripping on the 1st minimum DNBR value from the twelve on-line DNBR calculations using 2-out-of-4 C&I divisional voting when in-coincidence with a high SPND power density difference between symmetrical partners using 2-out-of-4 C&I divisional voting.
- Tripping on a high RCCA insertion or withdrawal rate using 2-out-of-4 C&I divisional voting.

81 Claims on the $DNBR_{low}$ trip parameter are currently made for three design basis faults (uncontrolled RCCA bank withdrawal at power faults, RCCA misalignment faults and uncontrolled single RCCA withdrawal faults) within the PCSR assessed during Step 4 of GDA (Ref. 22) although other faults use the parameter to demonstrate on-line compliance with the LCOs during normal operation. As seen above (Section 4.2.2), an additional claim is now being also made on this trip parameter for excessive increase in steam flow faults. However, of these, only the RCCA misalignment and single RCCA withdrawal faults result in asymmetrical flux distributions that derive the most benefit from the introduction of a protection system based upon in-core instrumentation. Reactor physics analysis studies that demonstrate the functionality of the SPND system for these faults assuming the worst single failure to meet the requirements of SAPs FA.6, EDR.2 and EDR.4 are referenced in the PCSR (Ref. 22) but these have not been assessed during Step 4 of GDA and in any case are not UK EPR™ specific. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-42** for a future licensee to provide UK EPR™ design specific calculations for the determination of the loss of accuracy factors applied to the trip set point for RCCA misalignment faults and uncontrolled single RCCA withdrawal faults so as to avoid DNB. As this is a first line trip parameter, the analysis will need to assume an un-revealed single failure in the most effective SPND finger to meet the requirements of SAPs FA.6, FA.7, EDR.2 and EDR.4.

82 My assessment of RCCA misalignment faults has illustrated the importance of the in-core SPNDs to the UK EPR™ safety case for such faults. The SPNDs are used:

- To demonstrate compliance with the initial LCO conditions.
- To activate the RCSL system to protect against the fault.
- To provide the $DNBR_{low}$ trip signal to protect against the fault.
- To protect against the fault for the ATWS situation associated with failure of the PS (through ensuring compliance with the initial LCO conditions).

83 Given the complexity of the processing equipment associated with the SPNDs as described above and the fact that RCCA misplacement faults are categorised as frequent faults, it is highly desirable to ensure some form of functional diversity is provided against an un-revealed common mode failure in the C&I processing equipment. One possibility would be to explore whether the operator can monitor changes in the axial offset values and quadrant tilts measured using the ex-core detectors to demonstrate that the reactor remains relatively well trimmed despite a potentially un-revealed common mode failure in the in-core instrumentation. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-43** for a future licensee to demonstrate that the ex-core detectors can be used to provide diverse protection by monitoring the axial offset during normal operation to ensure sufficient safety margin is available to avoid significant fuel damage and ideally DNB occurring during a dropped RCCA transient with an undetected common mode failure of the in-core instrumentation.

4.5.3 Findings

84 Following my assessment of the EDF and AREVA submissions, I am content for Action 5 of GDA issue **GI-UKEPR-FS-02** to be closed. I have raised two Assessment Findings **AF-UKEPR-FS-42** and **AF-UKEPR-FS-43**. Assessment Finding **AF-UKEPR-FS-42** requires a future licensee to provide UK EPR™ design specific calculations for the determination of the loss of accuracy factors applied to the trip set point for RCCA misalignment faults and uncontrolled single RCCA withdrawal faults so as to avoid DNB. Assessment Finding **AF-UKEPR-FS-43** requires a future licensee to demonstrate that the ex-core detectors can be used to provide diverse protection by monitoring the axial offset during normal operation to ensure sufficient safety margin is available to avoid significant fuel damage occurring during a RCCA drop transient with an undetected failure of the in-core detections processing equipment.

4.6 Diverse Protection against Loss of CVCS Faults (Action 6)

4.6.1 Summary of EDF and AREVA's Safety Case

85 This fault sequence involves the failure of the CVCS to increase the boron concentration of primary circuit following a spurious reactor trip. The increase in boron concentration is needed because following every reactor trip there is an eventual reduction in the shutdown margin of the reactor core due to the decay of xenon and the cooldown of the reactor.

86 EDF and AREVA have reviewed the UK EPR™ design and claim that should the operator fail to ensure the adequate shutdown margin following reactor trip then the source range detectors will detect the high flux levels and automatically actuate the Emergency Boration System (EBS) through the protection system.

87 EDF and AREVA conclude that on the basis of the functional analysis presented adequate protection is provided against the fault.

4.6.2 Assessment

88 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2), it was noted that while the EBS and the In-containment Refuelling Water Storage Tank (IRWST) systems provide diverse sources of borated water should the operator fail to ensure adequate shutdown margin using the CVCS, both these systems are also dependent upon operator action for actuation. Although the timescales are long (many hours) this implies a combined human reliability claim on the operator action of 1×10^{-7} per demand to meet the design basis target of SAP T.8. For this reason, Action 6 of GDA issue **GI-UKEPR-FS-02** was raised requesting EDF and AREVA to consider the feasibility of automatically actuating the CVCS system to inject borated water after every reactor trip and for the EBS to be automatically actuated following failure of the CVCS.

89 In response to Action 6 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed a functional analysis (Ref. 16) of the UK EPR™ design and claim that should the operator fail to ensure the adequate shutdown margin following reactor trip then the source range detectors will detect the high flux levels and automatically actuate the EBS through the protection system. To better understand the claim that is being made on the source range detectors TQ-EPR-1539 (Ref. 9) was raised requesting EDF and AREVA to confirm:

- That by the time the xenon level has decayed to its initial value the neutron flux level will have fallen sufficiently such that the permissive interlock on the source range detectors will have been lifted allowing them, rather than the intermediate range detectors, to monitor the neutron flux level.
- That the EBS is functionally capable of injecting borated water at a sufficient rate to overcome the rate of reactivity rise associated with the decay of xenon and the cooldown of the core once the actuation trip set point is reached.
- That the automatic actuation signal has an appropriate safety classification.

90 In their response (Ref. 26), EDF and AREVA confirmed that neutron flux levels at 16-20 hours after reactor trip will be range 10^{-10} to 10^{-8} of full power compared with the permissive set point of 10^{-6} to 10^{-7} demonstrating that the source range detectors will be operational. They confirm that the rate of boration required is 350 ppm/hr which is dominated by the cooldown rate rather than the xenon decay rate and that this is used to define a minimum EBS flow rate of 10 m^3/hr. They also confirm that the high neutron flux signal on the source range detectors is a RRC-A feature actuated through the PS designed to mitigate homogeneous boron dilution with failure of the dilution source isolation. In their response to TQ-EPR-1595 (Ref. 9) they provide further clarification that the EBS actuation via the protection system is Class 1. My judgement is that an adequate automatic means already exists for ensuring EBS actuation following failure of the CVCS on the UK EPR™ design. I am therefore satisfied that Action 6 of GDA issue **GI-UKEPR-FS-02** can be closed. There is no need for any additional assessment findings.

4.6.3 Findings

91 Following my assessment of the EDF and AREVA submissions, I am content for Action 6 of GDA issue **GI-UKEPR-FS-02** to be closed. There are no additional assessment findings.

4.7 Diverse Protection against Homogeneous Boron Dilution Faults (Action 7)

4.7.1 Summary of EDF and AREVA's Safety Case

92 This fault sequence involves a homogeneous boron dilution fault due a malfunction of the CVCS occurring while the reactor is shutdown together with a failure of the protection system to isolate the fault. Without mitigation such a fault can result in a return to criticality with potentially serious consequences.

93 The basis of the EDF and AREVA safety case is that they have performed an ALARP assessment (Ref. 17) and identified three potential solutions to provide a diverse engineered safeguard feature actuation signal to protect against a homogeneous boron dilution fault all of which at this stage could be reasonably practicable. Since all three options are potentially capable of detecting the fault EDF and AREVA have proposed that investigation of all three options should continue during the site specific detailed design phase.

94 EDF and AREVA consider that implementation of any one of the proposed design changes will provide adequate protection against the fault.

4.7.2 Assessment

95 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2), it was noted that a CVCS malfunction resulting in boron dilution fault during shutdown with the failure of the reactor PS to initiate anti-dilution protection needs to be considered within the safety case. Given that EDF and AREVA had not presented any analysis for this sequence, Action 7 of GDA Issue **GI-UKEPR-FS-02** was raised for such a safety case to be provided.

96 In response to Action 7 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed an ALARP assessment (Ref. 17) and identified three potential solutions to provide a diverse engineered safeguard feature actuation signal in the event of loss of TXS following a homogeneous boron dilution fault. The options identified are:

- Provision of an automatic high flux signal on a non-TXS based system from the existing source range detectors to isolate the CVCS and actuate the EBS system.
- Provision of an automatic low boron concentration signal on a non-TXS based system from the existing sampling line boronmeter to isolate the CVCS and actuate the EBS system.
- Provision of an automatic low boron concentration signal on a non-TXS based system from a new boronmeter located on either the CVCS letdown or charging line to isolate the CVCS and actuate the EBS system.

97 Since all three options are potentially capable of detecting the fault EDF and AREVA have proposed that investigations of all three options should continue during the site specific detailed design phase. For this reason, EDF and AREVA have raised CMF#59 (Ref. 8) to include completion of the ALARP assessment as part of the design change proposal.

98 In the following paragraphs, I briefly review each of these options.

99 The first option is to generate a high flux signal from the existing source range detectors. The ALARP review identifies that the response time of the detectors is fast and that it is already used to generate an alarm and automatic boron injection from the EBS. As it is utilised on the protection system all of the components need to meet the requirements for

a Class 1 system. As such there would be no impact on plant layout with the output signals just having to be duplicated on a non-TXS based system. EDF and AREVA state that exploratory analyses have been performed that demonstrate a momentary return to criticality and power which is terminated once the EBS injection becomes effective. It is claimed that the PCC-2 criteria for DNB and high linear power are met, although this work has not currently been independently assessed by ONR. However, EDF and AREVA note that for shutdown states there are difficulties related to the source range detector response due to variations in water density and core loading and it is very dependent upon the fuel management scheme, particularly the fuel assemblies adjacent to the detectors. This creates difficulties in determining the set point threshold to avoid spurious actuation and ensure that the core remains sub-critical. It is likely that this is not helped by the heavy reflector used on the UK EPR™.

100 The second option is to use the pre-existing sampling line boronmeter. This consists of a fission chamber and so is of a diverse design from the CVCS boronmeter. EDF and AREVA claim that the configuration is such that it can be used to sample all shutdown states. However, the response time of the system is 30 minutes but with the actuation signal being generated automatically. EDF and AREVA present analysis to argue that at least one hour is available before a return to criticality can occur providing a minimum ratio between the initial boron concentration and the critical boron concentration is observed during normal shutdown operation for a given CVCS charging rate. EDF and AREVA acknowledge that this will increase the required boron concentration in cold shutdown for certain limiting fuel cycles. I also note that this requirement would need to be captured as a Limit and Condition of safe Operation (LCO) within the technical specifications. This one hour margin would also not be available for mid-loop operations, although the assessment of this operating state is outside the scope of GDA. The active components of the boronmeter would also need to be upgraded from Class 3 to Class 2 with significant but feasible changes to the C&I. EDF and AREVA conclude that changes to plant layout would be less significant.

101 The third option is provision of a new boronmeter on either the charging or letdown line of the CVCS. The final choice will be a compromise between effect on transit time and layout impact. The response time of the detector is fast (1 minute). Location on the letdown line would increase transit time although this appears to assume the RCPs are not operating. As with the other options, the set point would need to take into account the operating state to ensure criticality is avoided while minimising the risk of spurious operation. The main concern appears to be with the impact on plant layout which is judged to be substantial in either location but with the letdown line being preferred. I potentially perceive an advantage with the letdown line in that the boron concentration of the RCS is being directly measured as opposed to the case of the charging line where the boron concentration being measured is that being injected from the CVCS.

102 All options require operator intervention in determination of the set point which is clearly an area of the safety case that will need detailed human factors justification. While the use of ex-core detectors has the advantage of directly measuring the flux transient the use of boronmeters has the potential to eliminate the fault earlier in a transient before criticality is even approached. In my judgement, significant progress has been made with the safety case for the purposes of GDA recognising that all options have the potential to produce an adequately safe outcome. I am therefore content to close Action 7 of GDA issue **GI-UKEPR-FS-02**. Assessment Finding **AF-UKEPR-FS-44** is raised for a future licensee to continue the development of the ALARP options to determine the optimum solution. Recognising that there are a number of potential solutions available, my

judgement is that resolution of this issue can be completed after the pouring of first nuclear (island) safety-related concrete.

4.7.3 Findings

103 Following my assessment of the EDF and AREVA submissions, I am content for Action 7 of GDA issue **GI-UKEPR-FS-02** to be closed. Assessment Finding **AF-UKEPR-FS-44** has been raised for a future licensee to complete and implement the ALARP assessment.

4.8 Diverse Protection for Loss of Essential Support System Faults (Action 8)

4.8.1 Summary of EDF and AREVA's Safety Case

104 In general, faults in this category result in the total or partial loss of one of the essential support systems on the reactor. These include loss of CCWS, loss of ESWS, loss of the CVCS, loss of HVAC systems and loss of electrical supply faults. Such faults can potentially produce multiple consequences. For example, the loss of the CCWS can result in the loss of cooling to the RCP seals causing a Small Break Loss of Coolant Accident (SBLOCA) and failure of cooling to the IRWST with consequential loss of the Medium Head Safety Injection (MHSI). However, in the context of demonstrating functional diversity for frequent faults for the purposes of Action 8 of GDA issue **GI-UKEPR-FS-02**, it is only necessary for frequent loss of essential support system faults to be considered.

105 The basis of the EDF and AREVA safety case is that they have reviewed a number of postulated events which they consider to be frequent design basis faults. These result in only the partial loss of essential support systems. For those cases which they consider to be limiting, they have performed a detailed functional analysis. EDF and AREVA claim that this analysis demonstrates, even for the most bounding faults, only one safeguard division will be lost such that adequate protection is provided even after considering an additional common mode failure of a front line system.

106 In the specific case of a Station Blackout (SBO) sequence involving a LOOP fault occurring together with failure of the EDGs, EDF and AREVA claim that the timescales are sufficient to ensure reliable manual actuation of the UDGs by the operator without the need for automatic actuation.

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

4.8.2 Assessment

108 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2), it was noted that EDF and AREVA were still in the process of developing a design basis safety case for a number of these systems. Given the importance of these systems, GDA issue **GI-UKEPR-FS-05** was raised requesting EDF and AREVA to provide a design basis analysis covering failure of the essential support systems. The assessment of the response to GDA issue **GI-UKEPR-FS-05** is reported in the associated close out report (Ref. 27) and is not discussed further here. However, EDF and AREVA were also asked that where any of these faults were frequent faults, they should in addition provide a demonstration of functional diversity under Action 8 of GDA issue **GI-UKEPR-FS-02**. Specifically, it was noted that LOOP together with common mode failure of the EDGs was not considered in the review of functional diversity for frequent faults. Given the timescales involved for operator action and the serious consequences should the operator

fail to perform the actions, EDF and AREVA were asked to look into the feasibility of automating the start-up of the UDGs from a diverse reactor protection system as part of Action 8 of GDA issue **GI-UKEPR-FS-02**.

109 In response to Action 8 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have identified (Ref. 18) the following loss of essential support system faults which they consider to be frequent initiating events:

- Mechanical failure of a single CCWS / ESWS train (together with an additional maintenance) with consequential loss of one safeguard building electrical and C&I division.
- Break in a single CCWS / ESWS train with consequential loss of thermal barrier cooling for four RCPs and loss of one safeguard building electrical and C&I division.
- Break in a single CCWS / ESWS common header with consequential loss of thermal barrier cooling for four RCPs and loss of one safeguard building electrical and C&I division.
- Loss of one train of the main safeguard building HVAC system (together with an additional maintenance) with consequential loss of one safeguard building electrical and C&I division.
- Loss of one safeguard building essential electrical switchboard with consequential loss of one safeguard building electrical and C&I division.

110 They conclude (Ref. 18) that the following two new frequent design basis faults bound these initiating events:

- Two tripped RCPs with loss of one safeguard building division.
- Four RCP seal LOCAs with loss of one safeguard building division.

111 The ONR assessment of the safety submission that identifies these events is presented in the close out report for GDA Issue **GI-UKEPR-FS-05** (Ref. 27) and is not discussed further here. However, EDF and AREVA acknowledge that these new design basis events are frequent and so they have analysed them for functional diversity to reach the controlled state (in response to Action 8 of GDA issue **GI-UKEPR-FS-02** discussed in the following paragraphs) and the safe shutdown state (in response to Action 9 of GDA issue **GI-UKEPR-FS-02** discussed in Section 4.9.2 below).

112 In the case of the two tripped RCPs with loss of safeguard building division, EDF and AREVA perform a review of the lower level safety functions and argue that the fault is bounded by the pre-existing diversity analysis for the partial loss of core coolant flow and forced decrease of reactor coolant flow design basis faults. In the case of four RCP seal LOCAs with loss of one safeguard building division, EDF and AREVA perform a review of the lower level safety functions and argue that the fault is bounded by the pre-existing diversity analysis for the SBLOCA design basis fault. In particular, EDF and AREVA confirm that each lower level safety function and safety feature group will still be available with one safeguard division lost. Since only one MHSI train, one Low Head Safety Injection (LHSI) train, one EFWS train, one MSRT train, and one EBS train are lost of the frontline systems as a result of the initiating event, I accept this argument. It should be noted that my assessment of faults that result in the loss of more than one safeguard division either due to an additional single failure and plant maintenance condition or due to the total loss of an essential support system is presented in the closeout assessment report (Ref. 27) for GDA issue **GI-UKEPR-FS-05**.

113 There is one aspect of the functional diversity review that is still not complete. In performing the functional diversity review for frequent faults during GDA Step 4, only the frontline systems were considered by EDF and AREVA as candidate systems for common mode failure. Common mode failure of an essential support system in-coincidence with a frequent initiating event was not considered. My judgement is that work performed in response to **GI-UKEPR-FS-05**, which has required EDF and AREVA to consider the total as well as the partial loss of each essential support system as initiating events, and which has resulted in a number of plant modifications, will also make the UK EPR™ robust to such common mode failures following frequent faults. The basis of my judgement is that most frequent faults are intact circuit faults such that once the reactor is tripped and all essential isolation functions have been performed by the protection system then the faults will essentially be equivalent to a fault initiated by common mode failure of an essential support system that results in a reactor trip. Such faults are covered in the analysis performed for **GI-UKEPR-FS-05** (Ref. 27) which considers common mode failure of the cooling chain, the main safeguard building HVAC system, and common voltage levels on the essential electrical system. The case of a frequent SBLOCA fault is also covered since the analysis in **GI-UKEPR-FS-05** for the total loss of cooling chain also assumes that a consequential seal Loss of Coolant Accident (LOCA) occurs while the aim of the design changes to the HVAC system and the essential electrical system is to ensure that all important front-line safety functions remain available following a common mode failure within these systems. An exception not covered by the **GI-UKEPR-FS-05** work is common mode failure of the four EDGs and the two UDGs following LOOP. Such a fault sequence initially results in the total loss of interruptible AC power (the battery backed uninterruptible AC power is assumed to remain operational). However, this sequence is explicitly discussed in the close-out report for GDA issue **GI-UKEPR-CC-03** (Ref. 28) covering lessons learnt from Fukushima. Assessment Findings **AF-UKEPR-CC-16** to **AF-UKEPR-CC-18** have been raised requiring a future licensee to considered design changes to improve the protection against such a fault sequence including consideration of a diverse means of providing emergency feedwater to the steam generators. In particular, Assessment Finding **AF-UKEPR-CC-17** specifically requests that consideration should be given to the use of steam turbines as a diverse means of achieving this function.

114 On the basis of the work performed in closing out GDA issues **GI-UKEPR-FS-05** and **GI-UKEPR-CC-03,** I am satisfied that Action 8 of GDA issue **GI-UKEPR-FS-02** can be closed. Nevertheless, there is a need for a demonstration of functional diversity in essential support systems following frequent faults to be formally demonstrated within the safety case. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-45** for a future licensee to perform a functional diversity analysis for all frequent design basis faults considering the common mode failure of each of the essential support systems to demonstrate that adequate functional diversity is provided.

115 As part of the response to Action 8 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed an ALARP review (Ref. 19) covering UDG actuation for the LOOP sequence associated with failure of the PS. In addition, they also consider mechanical failure of the EDGs sequence since this sequence would also be affected by any modification.

116 The report (Ref. 19) provides an overview of the design of the EDGs and UDGs noting that the former are Class 1 while the latter have been upgraded under CMF#37 to Class 2. The report then notes the measures taken in order to exclude the possibility of a common mode failure in both the EDGs and UDGs. These include being of a different design with different powers and voltages and independent support systems. In addition,

the start-up design for the EDGs is automatic while that for UDGs is through the SAS and is manual consistent with the design aim of EDF and AREVA that the UDGs should be simple and robust. The report then outlines the start-up procedure for the UDGs. This involves three grouped commands. The first cancels the existing orders from the PS and performs a load shedding operation of all non essential actuators. The second starts the UDGs. The third command reconnects and starts the EFWS and re-starts the ventilation systems. EDF and AREVA claim that the manual UDG start-up procedure is very simple as the operator executes grouped commands and that procedural safeguards are in place to ensure that the operator actions are executed in the correct sequence.

117 The report then provides an ALARP analysis. As noted above, EDF and AREVA consider the following two sequences:

- LOOP with failure of the PS (and consequential failure of the EDGs).
- LOOP with mechanical failure of the EDGs to start.

118 The sequence LOOP with PS failure bounds the sequence LOOP with mechanical failure of the EDGs since in the latter case, the PS ensures a prompt trip occurs after 2 seconds following loss of grid whereas the SAS actuates the reactor trip on high hot leg pressure after 9 seconds. Transient analysis results are quoted for providing the timescale of 42 minutes for the water level in the SGs to reduce to the 14% wide range level. For the mechanical failure this increases to 55 minutes. EDF and AREVA state (Ref. 20) that the 14% wide range level is identified in the current emergency operating procedures as when the operator should not re-start feed to an SG due to concerns over a thermal shock but does not necessarily correspond to a cliff-edge. In their response to TQ-EPR-1621 (Ref. 9) EDF and AREVA claim that this requirement does not need to apply to station blackout sequences and feedline break sequences, although no substantiating evidence is provided. Using the 0% wide range level, increases the time available to 58 minutes. They also claim that best estimate analysis based upon claiming the margins available regarding RCS inventory decrease through Pressuriser Safety Valve (PSV) opening leading to the core becoming uncovered increases this timescale to above 80 minutes (Ref. 20).

119 EDF and AREVA have performed a human factors assessment and argue that even allowing for the 30 minute rule in SAP ESS.9, the 42 minutes available is sufficient time to perform the action successfully. They add that at 58 minutes the operator reliability is 2×10^{-2} per demand and increases at 80 minutes to 2×10^{-3} per demand. EDF and AREVA acknowledge that the human reliability assessment for GDA is simplified due to the absence of procedures such that for timescales greater than one hour there tends to be a significant improvement in the predicted reliability. However, their judgement is that due to the extended timescales there is good opportunity for an operator to recover from a failure in an action to start a UDG such that during the site specific detailed design phase a probability of failure between 1×10^{-2} and 1×10^{-3} per demand is expected to be demonstrated. ONRs human factor specialists have assessed these submissions (Refs 13 & 29) and conclude that with further work during the site specific detailed design phase, EDF and AREVA should be able to demonstrate that an adequately reliable manual start-up can be achieved. It should be noted that in order to improve the human reliability claim on the UDGs, EDF and AREVA have simplified the start-up procedure by removing the requirement on the operator to first attempt to start-up the EDGs local to plant. While I can understand the logic for this decision it is not clear that the implications of this change to the safety case have been fully worked out. For example, the C&I documentation justifying the functional specification of the NCSS discussed in Section 4.14.2 still makes reference to transient analysis studies assuming all four EDGs

are available following LOOP with failure of PS/SAS. This may now be less likely and so there may be need for additional functionality on the NCSS to allow manual start-up of either the EDGs or the UDGs.

120 EDF and AREVA then performed an ALARP assessment (Ref. 19). They identify two ALARP options. The first option is to retain the current design. The second option is to automate the start-up of the UDGs on the SAS platform. Automating start-up of the EDGs on the SAS platform is rejected as it provides no benefit for the case of mechanical failure of the EDGs and means that the SAS system interfaces with both the EDGs and the UDGs potentially compromising diversity. EDF and AREVA then review the safety benefits of the two main options. They conclude that given the timescales available and the good reliability of the operator to perform the actions, the current option is to be preferred since it is more diverse and also avoids the need for providing a C&I system with the capability to automatically cancel the Class 1 signals from the PS.

121 It is noticeable that the stand-still seal system is being claimed to ensure that the primary circuit remains intact for this sequence. This is an F2 (or Class 3) system on the UK EPR™ that I would not expect to see claimed in a diversity assessment for frequent faults. Given its function to ensure that all four RCP seal remain leak tight it is my judgement that it must be potentially vulnerable to a single failure since it is a 4-out-of-4 system. While I would welcome EDF and AREVA providing further information to substantiate the design of this system (see below) I am keen to see arguments presented demonstrating that the safety injection system is functionally capable of providing make-up during the station blackout sequence. However, this requires knowledge on the loading of the UDGs that I feel is more appropriately explored in the context of general loss of electrical supply faults covered in close out assessment report (Ref. 27) for GDA issue **GI-UKEPR-FS-05**.

122 In conclusion, it can be seen that there is a significant amount of work still to be done to fully substantiate the safety case for the station blackout sequence. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-46** for a future licensee to provide a fully integrated safety case for the station blackout sequence. This will need to substantiate the claims on operator reliability, review the implications of prioritising UDG start-up over local to plant start-up of the EDGs, substantiate the timescales predicted from transient analysis studies, the structural integrity claims covering thermal shock following restart of feed to empty SGs, and the structural integrity and reliability claims on the stand-still seal system due to thermal and mechanical loads they experience during the fault sequence. Nevertheless, on the basis of the information presented, I am content that sufficient progress has been made for the purposes of GDA to justify the closure of Action 8 of GDA issue **GI-UKEPR-FS-02**.

4.8.3 Findings

123 Following my assessment of the EDF and AREVA submissions, I am content for Action 8 of GDA issue **GI-UKEPR-FS-02** to be closed. Assessment Findings **AF-UKEPR-FS-45** and **AF-UKPER-FS-46** have been raised. Assessment Finding **AF-UKEPR-FS-45** is for a future licensee to perform a functional diversity analysis for frequent faults considering the common mode failure of each of the essential support systems while Assessment Finding **AF-UKEPR-FS-46** is for a future licensee to provide a fully integrated safety case covering the station blackout sequence.

4.9 Diverse Means of Achieving the Safe Shutdown State (Action 9)

4.9.1 Summary of EDF and AREVA's Safety Case

124 During most design basis faults there is an initial period where safety limits (e.g. fuel safety limits, plant pressure limits, etc) are challenged while the safety systems are triggered and act to mitigate the fault. After this early period has passed and a controlled state (or non-hazardous stable state) has been reached where the three main safety functions, i.e. reactivity control, heat removal and containment are established, it is necessary to progress to a more long term sustainable condition known as the safe shutdown state.

125 The basis of the EDF and AREVA safety case is that following the establishment of the controlled state four actions are needed to reach the safe shutdown state. These actions are boration of the RCS, depressurisation of the RCS, cooldown of the RCS and connection of the Residual Heat Removal System (RHRS). EDF and AREVA then review each category of fault for all frequent faults to demonstrate that a diverse means exists to reach the safe shutdown state. In general the feed and bleed procedure is used in most cases to provide a diverse means of depressurisation, cooldown and boration. In other cases, it is demonstrated that the plant can remain in a final state for a long time.

126 EDF and AREVA conclude that on the basis of the functional analysis presented adequate diverse means is provided on the UK EPR™ to reach the safe shutdown state.

4.9.2 Assessment

127 In the GDA Step 4 Design Basis Faults Assessment Report (Ref. 2) it was noted that for frequent faults, EDF and AREVA had not provided a demonstration that a diverse means exists for moving from the controlled state to the safe shutdown state. For this reason, Action 9 of GDA issue **GI-UKEPR-FS-02** was raised for EDF and AREVA to provide such a safety case.

128 In response to Action 9 of GDA issue **GI-UKEPR-FS-02**, EDF and AREVA have performed a functional analysis (Ref. 21) to demonstrate that for frequent faults there is a diverse means of moving from the controlled state to the safe shutdown state. They make the assumption that the controlled state has been reached following an initiating event and that no failure of any system has occurred before that point apart from the initiating event itself. Consequently, the three main safety functions of reactivity control, heat removal and containment have been established. They then define four actions that are needed to reach the safe shutdown state from the controlled state. These are (not sequence):

- RCS boration
- RCS depressurisation
- RCS cooldown
- Connection of the RHRS.

129 EDF and AREVA then review each category of fault for all frequent faults to demonstrate that a diverse means exists to reach the safe shutdown state noting that connection of the RHRS is not strictly necessary to achieve a long term safe state. In their response to TQ-EPR-1579 (Ref. 9), EDF and AREVA clarify that there are three main safe shutdown states on the UK EPR™. These are:

- RHRS connection since one RHR train is sufficient to remove the residual heat at shutdown.

- Feed and bleed as demonstrated in transient analysis supporting the demonstration of functional diversity in Chapter 16.5 of the PCSR (Ref. 23) for the cases of SBLOCA fault with failure of the MSRTs and the total loss of feedwater fault.
- Heat removal via the secondary side with feed from two EFWS trains with replenishment of the feedwater tanks after 24 hours as demonstrated for the feedwater line break in Chapter 14.5 of the PCSR (Ref. 22).

130 Boration for the first two states is achieved using the Safety Injection System (SIS) / RHRS while for the third state it must be achieved using either the CVCS or the EBS. The response notes that these states are bounded by RRC-A analysis which are considered in the loading files to ensure the mechanical integrity of the components. On the basis of this response, I accept the EDF and AREVA definition of the three safe shutdown states. However, I do question whether the action to achieve adequate RCS boration needs to be performed earlier in order to reach a controlled state rather than the safe shutdown state.

131 In TQ-EPR-1569 (Ref. 9), EDF and AREVA acknowledge that only Category A functions should be used to reach the non-hazardous stable state in line with the requirements of IEC61226:2009. This standard defines the non-hazardous state as the “state of the plant where stabilisation of any transient has been achieved, the reactor is sub-critical, adequate heat removal is ensured and radioactive releases are limited. A transient is considered to be stabilised when, for all safety significant parameters, the margins (e.g. between the heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes.”

132 My interpretation of this definition is that following a successful reactor trip, the expected physical processes to be considered are the production of decay heat and the increase in core reactivity associated with the eventual decay of xenon and cooldown of the core. Hence the boration function is a Category A function that needs to be completed in order to reach the non-hazardous state. It would be unreasonably onerous to interpret the non-hazardous stable state as the long term safe shutdown state but it must at least correspond to the controlled state. This does imply the adequate RCS boration should be achieved in order to reach the controlled state.

133 In contrast, EDF and AREVA in their response to TQ-EPR-1569 (Ref. 9) appear to interpret this to mean that is not necessary to ensure that adequate boration of the RCS is achieved prior to reaching the controlled state. For this reason, I raised TQ-EPR-1595 (Ref. 9) requesting EDF and AREVA to confirm that the EBS can be activated by a Class 1 means for all design basis faults. They confirm that EBS actuation is via the protection system which is Class 1 and it can either be automatic or manual. I also asked for confirmation that the actuation of the SIS switchover to hot leg injection claimed for LOCA faults is Class 1. However, this was a manual action performed on the SAS at Class 2. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-47** for a future licensee to review, when preparing the response to cross-cutting Assessment Finding **AF-UKEPR-CC-01**, the definition of the controlled state against the definition of the non-hazardous stable state to ensure that the categorisation of the reactivity control function (and the classification of the associated safety systems provided to ensure adequate boration) is appropriate.

134 Once the controlled state has been reached, the minimum categorisation requirements reduce from A to B for the principal safety functions and from B to C for the diverse safety functions. Given that most frequent fault types are intact circuit faults, EDF and AREVA are able to argue that once the controlled state has been reached the reactor is already in a long term final state with SG feedwater supplied by the EFWS providing the feedwater

tank is replenished using the Class 3 fire water production system. A diverse path is provided by claiming the bleed and feed procedure using the SIS which is Class 1 and the PDS which is Class 2. The exceptions are SBLOCA, (Steam Generator Tube Rupture) SGTR and increase in heat removal faults.

135 For SBLOCA, EDF and AREVA argue that the boration function can be performed using the EBS or the feed and bleed procedure (assuming a small break) with SIS and PDS. RCS cooldown and depressurisation is performed using the MSRT to reduce SG pressure or the bleed and feed procedure. Should RHRS connection not be possible due to failure to stop the MHSI or due to failure to switch the LHSI to RHR mode, then the MHSI together with IRWST / CHRS are used to remove decay heat.

136 In the case of an SGTR fault, EDF and AREVA define that the controlled state is reached once the leak is compensated by the RCS water make-up. I do not agree with this definition. My definition would be that the SG flowrate is terminated with a pressure balance established between the RCS and the affected SG and that the affected SG is isolated. However, this concern is discussed further in the close out assessment report for GDA issue **GI-UKEPR-FS-04** covering the safety case for SGTR faults (Ref. 30) and so is not discussed further here other than to note that I have no concerns with the transfer to safe shutdown state for this fault once the controlled state has been reached.

137 Where an increase in heat removal fault is caused by a break in the secondary circuit it is necessary for the MSIVs to be isolated. In fact, in my judgement, this needs to be achieved to reach to controlled state rather than the safe shutdown state. The functional analysis (Ref. 21) states that no diversity is provided for common failure of the MSIVs. During GDA Step 4 (Ref. 2), EDF and AREVA did perform an ALARP assessment (Ref. 31) on whether there was a need for functional diversity to be provided for the MSIVs. However, the assessment only evaluated the benefits for an SGTR fault arguing this was the most bounding case. The need to isolate the four steam lines from each other to avoid an excessive cooldown fault was not discussed. Section 16.4 of the PCSR demonstrates that cooldown due to failure of the MSIVs on two main steamlines is acceptable but no assessment is given for failure of all four. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-48** for a future licensee revisit the ALARP assessment on the need for MSIV diversity and consider the increase in heat removal faults due to a break in the secondary circuit. There is need to see if one pair of steamlines can be isolated from the other pair or whether there is an adequate consequence case based upon SG nozzle limiting the rate of cooldown.

138 Finally, EDF and AREVA have also assessed the transfer to safe shutdown state for the case of frequent loss of essential support system faults. These faults result in the loss of one electrical and C&I safeguard division. In these circumstances EDF and AREVA argue (Ref. 18) that although one train is lost a diverse means of reaching the safe shutdown state is again provided by using bleed and feed with three SIS trains and the PDS valves. Should the LHSI be unavailable, then the CHRS can be used to remove the heat. EDF and AREVA claim that this system can operate with one train in conjunction with three MHSI trains, three MSRT trains and three EFWS trains.

139 This claim on the CHRS to cool the IRWST should the LHSI be unavailable is clearly important. During the GDA Step 4 assessment (Ref. 2), I noted that although EDF and AREVA have not considered the case within the diversity analysis, they have analysed the case within the RCC-A analysis. In the RCC-A analysis, EDF and AREVA claim that the safe shutdown state can be reached by using the Start-Standby System (SSS) or the EFWS, together with either the MSRT or MSB to provide a partial cooldown on the secondary side. The MHSI, accumulators and EBS are used to maintain sufficient water

inventory and to ensure the long-term control of reactivity on the primary side while the IRWST, CHRS, CCWS and ESWS are used to control the containment pressure and provide the ultimate heat sink. Through TQ-EPR-1579 (Ref. 9), I asked EDF and AREVA to confirm that the analysis provided still remains bounding for the UK EPR™ design. In their response, EDF and AREVA argue that the analysis remains bounding. Specifically with regard to the long term containment performance they report additional analysis carried out with an initial power of 4500 MW but with initial conditions in the containment, the residual heat and the functional capability of the CCWS / ESWS trains that they claim are conservative. EDF and AREVA claim the results demonstrate that the CHRS has sufficient capacity to extract the heat over the period 12 hours to 100 hours. However, the operator is assumed to actuate both CHRS trains rather than one. For this reason, I look further at the functional capability and sizing of the CHRS in the close out assessment report for GDA issue **GI-UKEPR-FS-05** (Ref. 27) covering loss of essential support systems.

140 Nevertheless, I am content with the demonstration of functional diversity to reach the safe shutdown state for frequent faults and judge that Action 9 of GDA issue **GI-UKEPR-FS-02** can be closed. My only concerns are associated with functions that are associated with reaching the controlled state rather than the safe shutdown state. I have raised Assessment Findings **AF-UKEPR-FS-47** and **AF-UKEPR-FS-48**. **AF-UKEPR-FS-47** covers the classification of the RCS boration function while **AF-UKEPR-FS-48** requires an ALARP assessment on the need for diverse means of isolating one pair of steam lines from the other pair following common mode failure of the MSIVs during a secondary circuit break.

4.9.3 Findings

141 Following my assessment of the EDF and AREVA submissions, I am content for Action 9 of GDA issue **GI-UKEPR-FS-02** to be closed. Assessment Findings **AF-UKEPR-FS-46** and **AF-UKEPR-FS-47** have been raised. **AF-UKEPR-FS-47** covers the classification of the RCS boration function while **AF-UKEPR-FS-48** requires an ALARP assessment on the need for diverse means of isolating the four steam lines from each other following common mode failure of the MSIVs during a secondary circuit break.

4.10 Minutes of the 10th UK EPR™ Design Safety Review Committee (8th February 2012)

142 During GDA, EDF and AREVA have commissioned independent peer reviews of individual chapters of the PCSR. Such reviews are called Independent Nuclear Safety Assessments (INSA). The results of an INSA are submitted for information and comment to the UK EPR™ Design Safety Review Committee (DSRC) which includes two independent members. The INSA of Chapter 16.5 of the PCSR which covers the demonstration of functional diversity for frequent faults on the UK EPR™ was submitted to the 10th meeting of the DSRC. Given the relevance of the subject to this assessment of GDA issue **GI-UKEPR-FS-02**, I have reviewed the minutes of the 10th meeting of the DSRC (Ref. 32). My observations are presented in the following paragraphs.

143 The minutes report one of the DSRC members as (correctly) noting that the review of functional diversity does not provide any information on cold-overpressure protection and whether there is a need for functional diversity. I share the members concern. The discussion of cold overpressure faults is presented in Chapter 5.2.4 of the PCSR covering structural integrity issues rather than Chapter 14 covering fault analysis. The PCSR explains that during cold shutdown states the PSV actuated by the PS are functional capable of providing cold overpressure protection. However, there is no discussion of the

frequency of the fault, whether it meets Plant Condition Category (PCC) analysis rules, or whether there is a need for functional diversity. In performing my assessment of actuator diversity, presented in Section 4.13.2 below, I compared the functionality of the SAS with the equivalent systems on Sizewell B. I note that Sizewell B claims a diverse spring loaded safety relief valve on the letdown line of the CVCS to provide diverse protection against cold overpressure faults. This suggests that there is probably a need for similar protection on the UK EPR™. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-49** for a future licensee to review whether there is a need for a diverse cold overpressure protection system to be provided on the UK EPR™.

144 A DSRC member makes a related comment that it is not clear the diversity analysis is complete for fault types from different plant states. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-50** for a future licensee to demonstrate the completeness of the diversity analysis for initiating events occurring from different plant states. The member also makes a specific comment in relation to providing a diverse means of ensuring feedwater isolation by tripping the main feedwater pump. This offers greater conceptual diversity to the main feed isolation valve than isolating the feed control valve as currently implemented on the UK EPR™. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-51** for a future licensee to perform an ALARP assessment into the feasibility of tripping the main feedwater pumps as a diverse means of ensuring feedwater isolation. Finally the DSRC also questions the rationale for excluding consideration of preventive maintenance within the functional diversity analysis. I raised similar concerns in Section 4.5 of the GDA Step 4 report (Ref. 2). While it is my judgement that this is unlikely to result in design changes, I do believe it is worth a future licensee reviewing the implications of considering plant maintenance on the diversity analysis unless it can be shown that the sequence frequency is clearly below the frequency cut off of 10^{-7} per year for design basis sequences. Such work needs to be performed in any case to support of the development of the future technical specifications for the UK EPR™. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-52** for a future licensee to perform such a review.

145 In summary, I conclude that the DSRC appears to have performed a useful challenge function in performing its review of Chapter 16.5 of the PCSR.

4.11 Review of the Update to the PCSR

146 The demonstration of function diversity for the UK EPR™ for frequent faults is presented in Chapters 14.7 and 16.5 of the updated PCSR (Ref. 21). These chapters were 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-02.**

147 In particular, I note the fault and protection schedule has been updated to reflect the change in classification of diverse systems of the following systems in accordance with CMF#36 and CMF#37:

- Upgrade to Class 2 of the actuation signal used for manually starting the Ultimate Diesel Generators (UDG).
- Upgrade to Class 2 of the actuation signal used for manually opening the Primary Depressurisation System (PDS).

- Upgrade to Class 2 of the actuation signal used for automatically closing the diverse full load Main Feedwater Isolation Valves.
- Upgrade to Class 2 of the Anticipated Trip without Scram (ATWS) signal used for the automatic actuation of the Emergency Boration System (EBS).
- Upgrade to Class 2 of the automatic CVCS charging pump switchover.
- Upgrade to Class 2 of the automatic diverse CVCS anti-dilution isolation.
- Upgrade to Class 2 of the manual start-up of the diverse third FPCS train.
- Upgrade to Class 2 of the Fuel Pool Cooling System (FPCS) purification pump trip.

148 In performing my assessment, I have become aware of the following areas that need to be updated in future updates to the site specific PCSR/POSRs:

- Chapter 14.0 still assumes that for faults involving the loss of a fuel pool cooling train the controlled state is reached at the start of the transient even though no engineered safeguards have been activated to protect against what is a design basis fault. Given that the main fuel pool cooling system has now been upgraded under CMF#38 to Class 1, there is neither a need nor technical justification for making this assumption.
- In the event of a fault on the CVCS following reactor trip, Chapter 14.1 and Chapter 16.5 both refer to the RCSL limitation function detecting a boron dilution fault and isolating the water source and actuating the EBS. EDF and AREVA have identified in their own response to TQ-EPR-1539 (Ref. 9) that the RCSL in fact actuates the reactor boron water make-up system rather than the EBS.
- In the analysis of spurious C&I signals reported in Chapter 16.4 the spurious opening of the MSRT case needs to be updated to reflect the fact that the low SG level reactor trip signal is no longer claimed as the diverse trip signal as noted in Section 4.2.2 above.
- A number of ATWS and RCC-A sequences appear in the fault schedule presented in Chapter 14.7. In principle, these sequences should be double accounting sequences that should already be presented in the diverse line for other faults. In general loss of support functions need to be included on the fault schedule. For example, the station blackout (SBO) sequence should be covered by an entry for LOOP and failure of main line (EDGs). I note that the stand-still seal system, which has safety classification of Class 3, is claimed as a diverse protection in the SBO sequence. This is not consistent with the commitment made by EDF and AREVA in response to **GI-UKEPR-CC-01** for all systems that provide diverse protection to be upgraded to at least Class 2. In addition, the long-term control of reactivity function is not presented in the fault schedule.

149 I have raised Assessment Finding **AF-UKEPR-FS-53** to cover the required updates to a site specific PCSR/POSR. In addition, there is a general need to update site specific versions of the PCSR including the fault analysis chapters and the fault and protection schedule 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**.

4.12 Assessment of Sensor Diversity

4.12.1 Summary of EDF and AREVA's Safety Case

150 Sensors and their associated conditioning modules are used on the UK EPR™ to measure key plant parameters and generate output signals which input into C&I safety systems. Given their crucial safety role, it is important to ensure that adequate diversity is provided within the sensors to enable the required design reliability targets to be met. For this reason, EDF and AREVA have decided to provide diverse sensors against all design basis faults with an initiating frequency greater than 1×10^{-3} per year.

151 The basis of the EDF and AREVA safety case is that they have reviewed each of these frequent initiating faults on a case by case basis and performed a functional analysis to demonstrate that adequate sensor types and conditioning module types are available to provide diverse protection.

152 EDF and AREVA conclude that an adequate demonstration of sensor and conditioning module diversity has been provided for the purposes of GDA recognising that further design work will be performed during the site specific detailed design phase.

4.12.2 Assessment

153 In response to the sensor diversity aspects of Action 9 of GDA Issue **GI-UKEPR-CI-06**, EDF and AREVA have provided a diversity implementation plan for sensors and conditioning modules (Ref. 33). This is supported by the following four key references:

- Safety Principles applied to the UK EPR™ I&C Architecture in terms of the requirements for Diversity and Independence (Ref. 34).
- Allocation of sensors & conditioning when three lines of defence are involved (Ref. 35).
- Diversity Criteria for Sensors & Conditioning (Ref. 36).
- Functional Analysis for Sensors' Common Cause Failure (Ref. 37).

154 In addition, during the close-out phase of GDA, EDF and AREVA have provided further technical justification through technical queries TQ-EPR-1555 and TQ-EPR-1578 (Ref.9) on the sensor diversity aspects. The response to TQ-EPR-1578 included the following document:

- Classification of I&C safety features (Ref. 38).

155 It should also be noted that the following information provided in support of the functional specification of the Non-Computerised Safety System (NCSS) in response to GDA Issue **GI-UKEPR-CI-01** (see Section 4.14.2) through TQ-EPR-1567 (Ref. 9) is also highly relevant and has been considered in the course of this assessment:

- Functional Requirements on Non-computerised safety I&C functions (Ref. 42).
- Comparison of the NCSS functions and SAS diversified functions (Ref. 45).

156 These documents taken together provide a reasonable overview of which sensors will be allocated to which of the three C&I safety system platforms (PS, SAS, NCSS) with the exception of the functional allocation of C&I systems for the support systems which have still to be determined.

157 The aim of the sensor and conditioning diversity implementation plan (Ref. 33) is to justify that adequate sensor and conditioning unit diversity is provided on the UK EPR™. In

order to achieve this, the diversity implementation plan (Ref. 33) applies the following five stage process:

- Determine the initiating frequency for which sensor and conditioning module diversity will be required on the UK EPR™.
- Identify the optimum strategy for allocating sensor and conditioning module types to the three safety system platforms (PS, SAS, NCSS) so as to minimise the number of diverse sensors and conditioning modules required.
- Define the engineering criteria to be used to determine when an appropriate amount of diversity has been achieved.
- Identify, on a fault by fault basis, for those initiating faults judged to require diverse sensors and conditioning modules, what diverse sensors and conditioning modules are provided on the UK EPR™ design.
- Based upon the fault by fault review, develop a diversity matrix summarising the provision of sensor and conditioning module diversity on the UK EPR™. Where shortfalls against the engineering criteria are identified an ALARP review is performed to identify improvements.

158 To achieve this, the implementation plan first references the C&I safety principles document (Ref. 34) covering requirements for diversity and independence. This identifies a number of principles covering the areas of defence in depth, independence, diversity, safety classification, fail safe design, and the human machine interface. Of these the defence in depth, independence and diversity requirements are relevant to sensor diversity. The requirements are slightly repetitive and so I précis them as follows:

- A preventive line of defence will be provided to control the main plant parameters and keep them within their required operating range assumed in the safety analysis. This line should be designed according to best-estimate design rules.
- A main line of defence will be provided to control the postulated initiating events of the design basis. The main line should be composed of a first line and a diverse line of protection for frequent initiating events with frequencies greater than 10^{-3} per year. The first line of protection should be designed according to conservative design rules. In particular, the design of the first line of protection should consider the single failure criterion, preventive maintenance, and the loss of off site power. These requirements are relaxed for the diverse line of protection.
- A risk reduction line of defence will be provided to control severe accident conditions. This line includes a back-up line (NCSS) to protect against initiating events with frequencies greater than 10^{-2} per year that are assumed to occur in coincidence with the failure of the computer based C&I systems. This frequency target aims at meeting the requirements of the Basic Safety Objective (BSO) target of SAP T.9 for an individual sequence assuming a common mode cut-off failure frequency for computer based technology of 10^{-6} per demand. This line should be designed according to best-estimate design rules.
- Independence and diversity will be provided between the lines of defence as far as is reasonably practicable to protect against common mode failure. This includes the C&I sensing, conditioning, processing and actuating equipment.
- Independence will be provided between the redundancies within a line of defence such that a single failure cannot result in the failure of the entire line of defence and

the failure of a lower classified component will not lead to the failure of a higher classified component.

159 Many of these principles are well established and consistent with the requirements of SAPs such as EKP.3, EDR.2, EDR.3, EDR.4, ESS.7, ESS.18, ESS.20 and T.9 that in my judgement are relevant to this issue. In the case of the numerical targets, the common mode cut-off frequency of 1×10^{-6} per demand proposed for computer based C&I systems is based upon a claimed reliability for the PS and SAS of 1×10^{-4} and 1×10^{-2} failures per demand respectively. The definition of frequent faults at 1×10^{-3} per year for which a diverse line of protection is required is consistent with relevant good practice in the UK. It is noticeable however that the requirements exclude consideration of the worst plant maintenance state. Given that the conditional probability for plant unavailability due to maintenance can be quite high, it is not clear that this is strictly adequate for very frequent events in the range 1×10^{-1} per year to 1×10^{-2} per year assuming a common mode failure cut off frequency of 1×10^{-4} per demand for the first line of protection when assessed against the BSO of 1×10^{-7} per year target in SAP T.8 for an individual sequence. In my judgement, there is a case for reviewing the implications of the worst plant maintenance condition on a fault by fault basis with regard to the strategy for allocation diverse conditioning module types which I discuss further below.

160 The next document (Ref. 35) considers the allocation of sensors between the three safety systems. It makes a simple probabilistic argument based upon the assumption that the common mode failure cut off frequency for a sensor/conditioning module type is in the range 1×10^{-4} to 1×10^{-5} per demand. Given that the equivalent numbers for the PS, SAS and NCSS are respectively 1×10^{-4}, 1×10^{-2}, 1×10^{-3} per demand it concludes that if only two diverse types of sensors or conditioning modules are available then the optimum strategy is to allocate one sensor/conditioning module type to the PS and the other sensor/conditioning module type to both the SAS and the NCSS so as to maximise the overall reliability. Otherwise three sensor/conditioning module types would be required to achieve the same level of reliability. Accepting that on a Pressurised Water Reactor (PWR) the number of well established means of monitoring conditions within the primary and secondary circuits are fairly limited, with most relying on the measurement of pressure either directly or indirectly (level measurement), my judgement is that the strategy is generally appropriate. However, it is noticeable that for very frequent faults, in the range 0.1 per year, the requirement on Sizewell B was for three sensors to be provided. I return to this point below when I perform a comparison of sensor provision on the UK EPR™ with that on Sizewell B.

161 Nevertheless, the approach has the merit in that it is easy to compare the functionality of the computer based SAS and non-computer based NCSS. Given that the role of both these systems is to provide diverse protection against failure of the computer based PS, comparison of the functionality between the SAS and NCSS indicates to what extent reliance is being placed solely upon computer based protection systems.

162 The next document (Ref. 36) defines the engineering criteria for assessing the quality of diversity achieved. In summary, it concludes that for sensors greater diversity is achieved if the two sensor types are based upon different measurement principles/physical effects applied to different reactor processes, with different manufacturers and whether they are located in different locations/fire zones. For conditioning modules greater diversity is achieved if the two module types are of a different design with at least one not relying upon software, with different manufacturers and whether they are located in different locations/fire zones. If all these criteria are met for a sensor or conditioning module then EDF and AREVA judged that “case 3” diversity is achieved. Lesser diversity is judged to

be “case 2” or “case 1”. “Case 0” corresponds to no diversity required. I accept that the more of these criteria that can be met, the better the diversity.

163 On the basis of the numerical targets identified in the C&I safety principles document (Ref. 34), a fault by fault review is performed in the functional analysis report (Ref. 37) covering common mode failure of sensors for all frequent faults using the fault schedule to identify for each front line safety function which sensors are applied to actuate a reactor trip, engineered safety feature, permissives, protection functions for the fuel building, and some of the support features. At some point the work will need to be extended to fully include support systems but it is recognised that this will have to await the completion of the work being performed under **GI-UKEPR-FS-05**. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-54** on functional diversity for a future licensee to extend the work performed to cover support systems. Nevertheless, in my opinion, the methodology is applied systematically and the result is a very useful report. In particular, the report identifies a number of modifications that need to be considered in the diversity implementation plan. These include diversified SG pressure sensors (CMF#67) and a general requirement to provide diverse pressure sensors (CMF#64).

164 The diversity implementation plan for sensors and conditioning modules (Ref. 33) draws the information from all these documents (Refs 34 to 37) together with the aim of establishing whether adequate diversity is provided on the UK EPR™. It presents an analysis that is performed in four stages. First it performs a reliability assessment of the sensors and conditioning modules to determine the minimum CCF cut off limit that needs to be achieved to ensure that the sensors and conditioning modules are sufficiently diverse so as not to limit the reliability of the protection systems when combined with the initiating event frequency of PCC-2 and PCC-3 events. From this EDF and AREVA conclude that for PCC-2 events “case 3” diversity is required for both sensors and conditioning equipment while for PCC-3 events “case 2” diversity is required for the sensors although “case 3” requirements are still required for the conditioning equipment. The second stage is to develop a diversity matrix based upon the fault by fault review of frequent faults (PCC-2 and frequent PCC-3 faults) (Ref. 37) to establish for each safety function (reactor trip or engineered safety feature) which sensors and conditioning modules need to be diverse. The results are summarised in Table 6 of the implementation plan (Ref. 33). The third stage is to review the current design against this diversity matrix to determine any shortcomings. The final stage involves identifying design solutions to overcome these shortcomings.

165 Although the overall approach seems appropriate, I had some concerns about the purely probabilistic approach in determining which cases can be “case 2” since it appears to preclude ALARP considerations of whether it is reasonably practicable to engineer the protection such as to ensure signal parameter diversity meets the “case 3” requirements which is clearly desirable from a safety perspective. In general, the aim of using PSA to balance the risks should be to identify areas of relatively high risk for further ALARP improvements and not as a justification to downgrade engineering requirements to a level determined by the highest risk from the dominant fault.

166 For this reason, I raised technical query TQ-EPR-1578 (Ref. 9) requesting EDF and AREVA to provide further justification of the approach adopted. EDF and AREVA were requested to justify that the list of frequent faults was complete, the list of sensors considered was complete, that sufficient diversity was provided for asymmetric faults affecting only one loop, and that “case 2” diversity was ALARP on a fault by fault basis for all cases where it is applied. In addition, EDF and AREVA were asked to justify that the

SPND in-core detectors and ex-core neutron flux detectors are adequately protected against common mode failure in the calibration of the detectors.

167 EDF and AREVA state that the list of faults is based upon PCC-2 and frequent PCC-3 events. However, the response acknowledges that the analysis presented in the implementation plan is not complete. Further work will be required on support systems, updates to the spent fuel pool safety case, frequent internal and external hazards, boron dilution faults and updates to the excessive increase in secondary steam flow faults. I expect as part of Assessment Finding **AF-UKEPR-FS-54**, for a future licensee to complete this work.

168 EDF and AREVA state that the list of sensors considered is based upon the claims in the fault schedule which they regard as a systematic approach to identifying sensors. However, to ensure no sensor is forgotten they have performed an additional review against the full list of sensors provided on the PS which is reported in the response to TQ-EPR-1578 (Ref. 39). In my judgement, this is a good approach to independently check the conclusions of the diversity plan. The report identifies a number of sensors associated with boron dilution faults, spent fuel pool faults, support system faults and internal flooding faults where the need for diverse sensors has not yet been considered which is to be expected given that these faults have been identified above as needing further consideration.

169 For some sensors (Main Steam Relief Isolation Valve (MSRIV) closed, RPV level, hot leg pressure narrow range (NR)), EDF and AREVA claim that the sensor is to advise the operator during emergency operations for which either other diverse sensors already exists or for which the event is infrequent. In the case of the intermediate power range detector, EDF and AREVA argue that the power range detectors provide a diverse sensor. This later claim will be confirmed when Assessment Finding **AF-UKEPR-FS-15** is closed out during the site specific detailed design phase.

170 EDF and AREVA argue that the other sensors only provide protection against infrequent faults for which diverse sensors are not required. These include sensors to protect against ATWS events, RCCA ejection faults, small break LOCAs in state B (hot shutdown conditions), breaks in the residual heat removal system during shutdown, total loss of cooling chain, station blackout, fuel and reactor building containment during fuel handling operations based upon fuel activity measurements, isolation of interfacing LOCA associated with the RCP thermal barrier failure, and containment isolation functions based upon containment pressure. I agree that most of the faults listed are infrequent but note that there is operational experience of small break LOCAs occurring on RCP thermal seals suggesting these should be considered frequent faults. However, I recognised that there are other sensors to protect against SBLOCA faults. There are also other sensors that will detect faults (SBLOCA, Steam Line Break (SLB)) that result in high containment pressure.

171 EDF and AREVA identified four faults that result in asymmetric fault conditions affecting only one loop. These are:

- Cooldown faults affecting one SG (increase in feed flow, small steamline or feedline break, inadvertent opening of an MSRT or MSSV).
- Single MSIV closure fault
- Single RCP trip fault
- SGTR fault

172 To provide better protection against cooldown faults after reactor trip, EDF and AREVA have decided to provide a new Class 1 diverse SG pressure signal under CMF#67. On each steamline four additional pressure sensors (type B) of a diverse design will be added to the four pressure sensors (type A) that already exist as shown on page C2 of the functional analysis report (Ref. 37). The intention is that the type A sensors will input into the PS and type B sensors into the SAS/NCSS. Sizewell B also claims that using pressures sensors of different design (strain gauge type and linear variable differential transformer type) provides adequate diversity so the proposal is not novel and represents accepted good practice. The reason for this proposal is that following reactor trip, MSIV isolation occurs on low SG pressure with a back-up provided by low cold leg temperature. For more benign cooldown faults, the cooldown is not sufficient to provide a low cold leg temperature signal and so the new low SG pressure signal provides the diverse signal required. Should MSIV isolation not terminate the cooldown then the operator is expected to isolate the affected SG by closing the MSRT and isolating feed using the pressure sensors to identify the affected SG. EDF and AREVA argue that SG pressure is the only realistic sensor for performing this operation which is why they are proposing the diverse pressure sensor.

173 The inadvertent closure of one MSIV leads to a fast increase in SG pressure which triggers a reactor trip. The new diverse pressure sensor provides diverse protection. EDF and AREVA were questioned about the possibility of using limit switches to detect the closure of an MSIV as applied at Sizewell B. However, they were reluctant to pursue this option because of concerns over the likelihood of a spurious reactor trip. This matter is discussed further below.

174 EDF and AREVA argue that although the loss of one RCP pump is an asymmetric fault it directly affects the whole reactor core. I accept this argument.

175 The last fault is a SGTR fault. Before discussing this fault it is necessary to point out that in addition to a diverse set of SG pressure sensors, EDF and AREVA are also proposing providing a diverse set of pressure sensors for the SG level narrow range and SG level wide range sensors. This is similar to Sizewell B. However, unlike Sizewell B, EDF and AREVA are proposing to split the sensor types so that two SGs have narrow range (NR) sensors type A and wide range (WR) sensors type B and two SGs have narrow range (NR) sensors type B and wide range (WR) sensors type A. While this is clearly adequate at least for reaching the controlled state for symmetric faults such as loss of feed, it means that for a single SGTR fault there is only a single sensor design available to generate a reactor trip on low SG level (NR). There is a 50% chance that the pressuriser pressure and level sensors will also be of the same design and so not diverse. This was the concern that motivated my question about asymmetric faults. However, for SGTR faults EDF and AREVA argue that the new Class 1 steamline activity sensors with manual trip developed under CMF#22 (Ref. 8) provide diverse protection against this fault.

176 There is also a concern about the ability to provide adequate post-trip cooling given the split in SG level sensors if the plant maintenance is assumed to occur on one of the EFWS pumps. This is because as the response to TQ-EPR-1555 makes clear, only the low SG level (WR) sensors on the SG associated with an EFWS pump can actuate that particular pump. Currently, to reach the long term safe shutdown state on the EPR it is necessary to ensure feed is provided to two SGs. Hence common mode failure of one sensor type coupled with a plant maintenance condition would result in insufficient feed being provided to the SGs. EDF and AREVA have confirmed that the need to feed two SGs is only to reach the long-term safe shutdown state. One SG is adequate to reach the controlled state. I also note that there is always the possibility for the operator to perform

a bleed and feed operation in such a situation. Overall, based upon the responses provided by EDF and AREVA, I am content that the proposed sensor split provides adequate protection.

177 In response to the question on "case 2" diversity, EDF and AREVA identified twenty-five cases where further justification was required and have incorporated this response into the final version of the diversity implementation plan (Ref. 33). In my opinion these cases can be rationalised down to the following eight combinations of sensors:

- Pressuriser pressure and hot leg pressure
- SG level (NR) and SG level (WR)
- Low DNBR and hot leg pressure (where the DNBR parameter is based on pressuriser pressure, SPND detectors, core inlet temperature, and core inlet flow)
- SG pressure and diversified SG pressure
- Loop level and diversified loop level
- Power range detector (PS) and power range detector (SAS/NCSS)
- RCP speed and RCP speed
- Steamline activity and SG activity

178 Each of these combinations is reviewed in the following paragraphs.

179 Low pressuriser pressure and low hot leg pressure are claimed to provide diverse reactor trip signals for SBLOCA and CVCS malfunction faults resulting in a decrease of RCS inventory and for safety injection, containment isolation and partial cooldown for small steamline break faults and excessive increase in secondary steam flow faults. Similar signals are claimed for Sizewell B. However, Sizewell B also has a diverse safety injection signal resulting in reactor trip based upon high containment pressure. I also note that although a low cold leg temperature signal is provided on the UK EPR™, the SAS is not capable of using it to initiate safety injection unlike the group 2 parameters on the PPS for Sizewell B.

180 High pressuriser pressure and high hot leg pressure are claimed to provide diverse reactor trip signals on turbine trip faults, loss of condenser faults, spurious pressuriser heater faults, and CVCS malfunctions resulting in an increase in RCS inventory. Similar signals are claimed for Sizewell B. However, Sizewell B also has an extra reactor trip based directly upon the turbine trip signal. This is probably because for very frequent faults (0.1 per year) Sizewell B had a rule that three diverse sensors have to be available. EDF and AREVA claim that use of the turbine trip signal to generate a reactor trip is avoided on the UK EPR™ because they want the load reduction limitation function on the RCSL system to provide protection against this fault. The assessment of the RCSL system is outside the scope of the fault studies assessment for GDA. Nevertheless, the RCSL system is a Class 2 system based on the Teleperm XS platform with a 1×10^{-2} failure per demand/failure per year reliability claim. The system is independent of the safety systems and diverse from the SAS/NCSS. However, EDF and AREVA will need to demonstrate that it is sufficiently independent so as to provide a risk reduction worth comparable to that of the turbine trip signal on Sizewell B.

181 Low SG level (NR) and low SG level (WR) are claimed to provide diverse reactor trip signals for loss of feed faults, feedline break faults, and for steamline break/excessive increases in steamline flow faults. They are also used to actuate the EFWS and isolate the SG blowdown system for intact circuit faults in general. The claim on SG level for

steamline break/excessive increases in steamline flow faults will need to be reviewed in the light of the Assessment Finding **AF-UKEPR-FS-41** that I have raised in Section 4.2.2 above when closing out Action 2 of GDA issue **GI-UKEPR-FS-02**. Otherwise this is similar to Sizewell B.

182 High SG level (NR) and high SG level (WR) are claimed to provide diverse main feedwater isolation signals for spurious increase in feed faults. This is similar to Sizewell B (Sizewell has two diverse SG level (NR) signals).

183 Low DNBR and low hot leg pressure are claimed to provide diverse reactor trip signals for spurious pressuriser spray faults. This is similar to Sizewell B (Sizewell is provided with an RCS (NR) pressure signal).

184 Low DNBR and high hot leg pressure are claimed to provide diverse reactor trip signals for slower uncontrolled RCCA bank withdrawal faults at power. This is similar to Sizewell B.

185 Low SG pressure and low diversified SG pressure are claimed to provide diverse MSIV isolation signals for steamline break/excessive increases in steamline flow faults. They are also claimed to isolate the MSRT. Although it is not formally claimed in the diversity analysis, the response to TQ-EPR-1578 (Ref. 39) claims that the low cold leg temperature signal can also isolate the MSIVs on the UK EPR™.

186 High SG pressure and high diversified SG pressure are claimed to provide diverse reactor trip signal following spurious closure of one or more MSIVs. As noted above, Sizewell B uses limit switches to measure MSIV position. However, my judgement is that the high hot leg pressure trip signal on the SAS coupled with the mechanically operated MSSVs and PSVs will also provide adequate diverse protection against this fault. Given the concerns of EDF and AREVA over spurious reactor trip signals discussed above, the current design is judged to be acceptable.

187 Low loop level (digital) and low loop level (analogue) are claimed to provide diverse safety injection and CVCS isolation signals following a LOCA during shutdown conditions. Sizewell B now uses ultrasonic sensors which are temporarily installed during outages to provide a diverse signal. This is probably worthwhile doing on the UK EPR™. However, this is an operational issue that can be resolved during the site specific detailed design phase.

188 In an earlier version of the functional analysis report (Ref. 37) a high flux signal on the Power Range Detector was initially claimed to provide a diverse reactor signal against itself for faster uncontrolled RCCA bank withdrawal faults at power. Subsequently, EDF and AREVA have argued that such fast faults are infrequent such that diversity is not required. In my judgement this claim is likely to be confirmed when the work for **AF-UKEPR-FS-15** is competed during the site specific detailed design phase although it is noted that Sizewell B is provided with a diverse set of ex-core detector designs.

189 Low RCP speed (PS) and low RCP speed (SAS) are claimed to provide diverse reactor trip signals for reduction in flow faults. However, the TQ-EPR-1578 (Ref. 39) response also notes that a low coolant flow rate signal using the pressure drop across the RCPs is also available. This is similar to Sizewell B. Again, because a short-term loss of grid fault is very frequent, Sizewell requires an additional set of sensors. Low RCP voltage and low RCP current are used as diverse signals to protect against this fault. During the site specific detailed design phase, a future licensee will therefore need to demonstrate with reference to the PSA that the risk from such a fault is sufficiently small in order to justify not providing these additional sensors.

190 High activity signal on the SG steamline and high activity signal on the SG secondary sampling system are claimed to provide alarms to prompt the operator to trip the reactor. EDF and AREVA note that the design of the sensors is of a diverse design and they are located in different locations. One sensor measures N-16 activity in the steamline. The other sensor measures fission and corrosion product activity in the liquid phase of the steam generator. For a single SGTR fault to escalate into a more serious fault it is necessary for either the CVCS or the feedwater control system to fail to operate correctly. In such circumstances, the reactor will automatically trip on either high SG level or low pressuriser level (or pressure), which therefore provides diverse protection against this fault. For this reason, I judge that adequate diversity is provided for this fault.

191 Recognising that the SPND and ex-core power range neutron flux detectors are intended to be diverse I requested EDF and AREVA to explain how they protect against common mode failure in the calibration of the detectors. In their response to TQ-EPR-1578 (Ref. 39), EDF and AREVA state that aero-ball measurement system (AMS) together with a theoretical core model allows a fine core power distribution called a flux map to be developed. This flux map is created and used off-line by station physicists performing core physics tests in accordance with procedures with step-by-step validation. These tests allow periodic checking of the core conformity after each reload and during the cycle and the periodic calibration of C&I signals such as high linear power and low DNBR trips. EDF and AREVA also noted that the diversified reactor trip signal on the ex-core detectors can be calibrated using the reference heat balance which does not rely on the AMS. This is considered a satisfactory response given that similar arrangements apply at Sizewell B for the calibration of the ex-core detectors.

192 From the above review I have concluded that there is a need for a future licensee to review whether it is ALARP to provide the following sensor input on the SAS:

- High containment pressure signal to generate safety injection (and reactor trip);
- Low cold leg temperature signal to generate safety injection (and reactor trip);
- A turbine trip signal to cause a reactor trip;
- Low RCP current to generate a reactor trip;
- Low RCP voltage to generate a reactor trip (possibly on the PS);
- Low SG pressure signal to generate a reactor trip;

193 In my view it is important that in performing the review, the licensee develops a PSA model to accurately represent the detailed allocation of sensor equipment. In addition, it must be noted that there are a number of areas where further work will be needed during the site specific detailed design phase. This includes providing justification for those functions on the SAS and NCSS for which it is proposed that reliance will be placed upon manual action. In addition, further transient analysis studies will be required covering the loss of one reactor coolant pump and the uncontrolled single RCCA withdrawal fault. I have raised Assessment Findings **AF-UKEPR-FS-55** to **AF-UKEPR-FS-64** for a future licensee to complete this work.

194 With regard to the allocation of diverse conditioning modules I have a concern that the allocation of conditioning modules is not always taking into account the implications of diversity claims within the safety case and particularly plant maintenance conditions. The response to TQ-EPR-1555 (Ref. 9) covering the allocation of conditioning modules to the SPND in-core neutron detectors and ex-core neutron detectors illustrates this concern. These detectors operate on a 2-out-of-4 voting system and are intended to be diverse. EDF and AREVA proposed that the allocation of conditioning modules should be split

such that the two types on module are each allocated on two out of the four outputs from each set of sensors. Hence, common mode failure of one set of sensors coupled with a plant maintenance condition on one of the C&I divisions associated with the conditioning modules would render both sets of flux protection unavailable. I consider it is ALARP to do better than this.

195 The reason for EDF and AREVA proposing this solution was because both sets of flux detectors were also meant to be diverse to hot leg pressure and so they had a combination of three diverse sensors and only two conditioning module types. In response to ONR concerns the latest proposal (Table 14, Ref. 33) is to allocate to both flux detectors the same conditioning modules in order to be diverse from the hot leg pressure since the fault that they were both claimed to be diverse for (Uncontrolled RCCA bank withdrawal at power (URBWP) – faster transient) is now argued to be infrequent. However, this ignores the fact that there is one other fault for which the flux detectors are claimed to be diverse which is not currently included on the fault schedule because the work on excessive increase in steam flow performed in response to Action 2 of GDA Issue **GI-UKEPR-FS-02** discussed in Section 4.2.2 above has identified that the ex-core detectors are needed to provide diverse protection to the low DNBR trip which is based upon the in-core detectors. In my opinion, the solution to this problem may be to claim extra trip parameters for the URBWP – slower fault transient (pressuriser pressure) and on the reduction of feedwater temperature fault (low DNBR trip). This problem is for a future licensee to solve. I have therefore raised Assessment Finding **AF-UKEPR-FS-65** for a future licensee to perform a further review of the allocation of conditioning modules for the in-core and ex-core flux detectors.

196 I believe this concern is a specific example of a broader concern that the precise distribution/allocation of conditioning modules to individual sensors and C&I safety system platforms needs further optimisation to ensure that maximum benefit is made of the diverse designs. In particular, I consider that PSA support is essential in ensuring that the number of lower order cut-sets is minimised, particularly after taking account of plant maintenance states on C&I divisions and safety system trains associated with 2-out-of-4 success criteria. For these reasons, I have raised Assessment Finding **AF-UKEPR-FS-66** for a future licensee to perform a further general review of the allocation of conditioning modules after developing a detailed fault tree model of the protection system. This work will also need to justify excluding consideration of the most onerous plant maintenance state within the safety principles (Ref. 34) applied to the UK EPR™ C&I architecture.

197 In addition to their responses to TQ-EPR-1578, EDF and AREVA have provided the current classification of C&I safety functions (Ref. 38) although the document recognises that it is a snapshot of the current design and will need updating during the site specific detailed design phase to include further changes identified during GDA including the response to GDA issue **GI-UKEPR-FS-05**. This document presents the functional allocation in a series of tables which are listed below.

- Table 1 – preventative line – RCSL Class 2/3 and the Process Automation System (PAS) – Class 3.
- Table 2a – first line – to reach the controlled state – Class 1.
- Table 2b – first line – to reach safe shutdown state – Class 2.
- Table 3a – diverse line – Class 2.
- Table 3b – diverse line – Class to be confirmed during the site specific detailed design phase.

- Table 3c – diverse line – Class to be confirmed during the site specific detailed design phase.
- Table 4 – back-up line – NCSS – Class 2 and a probabilistic line the class of which is to be confirmed during the site specific detailed design phase.
- Table 5 – Severe accident line – Class 3.

198 Although the document is a significant improvement on earlier versions, there are still some significant updates to be performed including incorporating the design implications of GDA Issue **GI-UKEPR-FS-05**. In particular, the document claims that the improvements and modifications associated with CMF#36 requiring that diverse lines of protection be safety classified to at least Class 2 have already been incorporated. However, Tables 3b and 3c list a considerable number of features that are still currently at Class 3. For example, automatic MHSI injection on low hot leg pressure is claimed in sub-section 3.3.2.3 of Chapter 16.5 of the PCSR as diverse protection for SBLOCA faults associated with failure of the reactor protection system. However, it still appears in Table 3b as a Class 3 system. It is also noticeable that some features that are listed in Table 2b as required for reaching the safe shutdown state are really diverse lines of protection. For example cooling of the LHSI and MHSI pump rooms appears in both Tables 2a and 2b. The Table 2a signal is allocated to the PS and is the first line of protection. The Table 2b signal, which starts on high temperature, is allocated to the SAS and appears to perform a diverse safety function suggesting it should really be in Table 3a. It is worth noting that Table 2b lists a large number of Class 2 HVAC systems that appear to support Class 1 functions. It also contains the SG water level control system for the EFWS at Class 2. Justification is required that this is adequate given that the EFWS performs a Class 1 function. Given these comments, I have raised Assessment Finding **AF-UKEPR-FS-67** requiring a future licensee to review the classification of C&I safety features document (Ref. 38) during the site specific detailed design phase.

199 Nevertheless, taken together with the results of the studies performed in support of developing the functional specification of the NCSS (Refs 42 & 45) and not withstanding the above concerns about classification, the document provides a reasonable overview of the C&I functional coverage on the UK EPR™. I have performed a high level comparison of the functionality against that provided on Sizewell B. The coverage provided appears to be broadly equivalent, particularly if the functions on the PS/SAS on the UK EPR™ are compared with the PPS group 1/group 2 parameters on Sizewell B and the functions on the NCSS on the UK EPR™ are compared with the SPS on Sizewell B although fewer automatic functions are provided on the UK EPR™ particularly for the NCSS. My judgement is that although the UK EPR™ has only one group of parameters provided on the PS system, this is compensated by the provision of the SAS system such that my overall judgement is that from a functionality point of view the C&I protection systems provided on the two reactor designs are broadly comparable. In particular, apart from those specific items already listed above, the signals provided for the reactor trip function although obviously different in detail are nevertheless judged to be broadly equivalent. For example, for faults occurring at power, Sizewell B has a diverse set of ex-core detectors and N-16 detectors while the UK EPR™ has ex-core and in-core detectors. Sizewell B has steamline pressure negative rate trip while the UK EPR™ has an SG pressure drop trip. For faults occurring during shutdown operation, Sizewell B has a diverse set of source range detectors while the UK EPR™ has a source range detector and boron meter on the PS with either an additional boron meter or an additional source range detector signal on the SAS. This gives me confidence that the overall balance of

sensor coverage on the three C&I systems and the overall number of diverse sensors provided by EDF and AREVA on the reactor primary and secondary circuits inside containment is adequate.

200 There is one area where there may be a need for temporary additional diverse sensors and this is to protect against core misloading faults since the in-core instrumentation is disconnected when the head package is removed for refuelling. However, this issue is already covered by the Step 4 Assessment Report for fuel and core design (Ref. 40) where Assessment Finding **AF-UKEPR-FD-03** has been raised for a future licensee to ensure that all practical measures are taken to avoid an uncontrolled criticality.

4.12.3 Findings

201 Overall, I am content that sufficient progress has been made with the diversity implementation plan covering the allocation of sensors to justify the closure of Action 9 of GDA issue **GI-UKEPR-CI-06** from a fault studies perspective.

202 With regard to the diversity implementation plan for sensors and conditioning modules, I am content that the allocation of one set of sensors to the PS and another set of diverse sensors to the SAS/NCSS is appropriate and logical when judged from a probabilistic perspective. I also judge that the overall balance of sensor coverage on the three C&I systems and the overall number of diverse sensors provided is adequate. However, I believe that there may be a case for using existing sensors to provide extra sensor inputs onto the SAS system and that additional justification is needed about the sensor coverage for initiating events with very high initiating frequencies so as to ensure that the PSA risk targets are met. Furthermore, I believe the precise distribution/allocation of conditioning modules to individual sensors and C&I safety system platforms may need further optimisation to ensure that maximum benefit is made of the diverse designs. In particular, I consider that PSA support is essential in ensuring that the number of lower order cut-sets is minimised particularly after taking account of plant maintenance states on C&I divisions and safety system trains associated with 2-out-of-4 success criteria. For these reasons, I have raised Assessment Findings **AF-UKEPR-FS-54** to **AF-UKEPR-FS-67** on the diversity of sensors and conditioning modules.

203 While I have raised fourteen Assessment Findings in this area, I am confident that these are resolvable during site specific detailed design phase and should not have any impact upon plant layout. In particular, I am now confident that EDF and AREVA have provided sufficient numbers of diverse sensor types on the reactor primary and secondary circuits. For this reason, I am satisfied that Action 9 of GDA issue **GI-UKEPR-CI-06** can now be close.

4.13 Assessment of Actuator Diversity

4.13.1 Summary of EDF and AREVA's Safety Case

204 Priority Actuation Controller System (PACS) modules are used on the UK EPR™ as the interface between the C&I safety systems and the mechanical actuators for front line plant systems. Given their crucial safety role, it is important to ensure that adequate diversity is provided within these actuators to enable the required design reliability targets to be met. For this reason, EDF and AREVA have decided to provide two diverse PACS module designs. The aim is to ensure diverse protection is provided against all frequent design basis faults with an initiating frequency greater than 1×10^{-3} per year.

205 The basis of the EDF and AREVA safety case is to generically allocate the PACS module types by division with divisions 1 & 2 getting type A PACS modules and divisions 3 & 4 getting type B PACS modules. EDF and AREVA have then reviewed each frequent initiating fault on a function by function basis to confirm that adequate PACS module diversity is provided. EDF and AREVA conclude that an adequate demonstration of PACS module diversity has been provided for the purposes of GDA recognising that further design work will be performed during the site specific detailed design phase.

4.13.2 Assessment

206 In response to the PACS module diversity aspects of Action 9 of GDA Issue **GI-UKEPR-CI-06**, EDF and AREVA have provided a diversity implementation plan for the PACS modules (Ref. 41) with the aim of determining the optimum distribution of PACS modules given that it is proposed to only have two diverse designs of PACS module. The generic approach adopted by EDF and AREVA is to allocate PACS module types by division and then check on a function by function basis using the fault schedule to determine that the impact of a common mode failure of one type of PACS module is acceptable. If not, a specific allocation is proposed.

207 As noted above, the generic allocation is that divisions 1 & 2 get type A PACS modules and divisions 3 & 4 get type B PACS modules. This solution is proposed on the grounds that diversification between the first and second lines presented in the fault schedule with just two PACS designs is difficult because of the different combinations of frontline systems. The example quoted is the SGTR fault and the excessive increase in secondary steam flow fault. The SGTR fault is a frequent LOCA event for which MHSI is claimed as the frontline system and LHSI as the diverse line. The excessive increase in secondary steam flow fault is a frequent intact circuit fault for which the diverse line is bleed and feed that is claimed to require both the MHSI and LHSI. I am not convinced by this argument and believe there is scope for allocating the modules to be consistent with diverse safety functions accepting that there is no need for a rigid generic solution to be applied in which all first line systems have one PACS module and all diverse line systems have another. A case by case approach can be adopted. To consider the example quoted, my judgement is that the MHSI and LHSI could and probably should be allocated diverse PACS modules to cover the LOCA case as they provide a diverse means of safety injection. However, I suspect that both are not needed for the bleed and feed case (which is in any case just a manually induced LOCA event). The EDF and AREVA C&I designers need input from their fault analyst colleagues to better understand for which systems diversity is essential rather than just desirable. The fault schedule is only a summary of the safety case and does not by itself provide sufficient information to determine the relative importance of each safety function. In particular, no input is provided from the PSA. In my opinion it is essential that the C&I processing equipment is modelled to confirm that the optimum selection is made with regard to the allocation of PACS modules.

208 A particular instance highlights my concerns. The list of functions in Section 6.3 of the diversity implementation plan (Ref. 41) states that a number of functions are 2-out-of-4 systems. These include EFWS, MHSI, and SG pressure control using the MSRT. No reference is given as to how these 2-out-of-4 requirements were determined. Given that the common mode failure limit for a PACS module is 10^{-5} per demand the need for 2-out-of-4 trains of these systems to be available for these sequences appears quite onerous to reach the controlled state given that the initiating event is a frequent fault that is generally associated with more benign fault transients. Nevertheless, taking the success criteria as they are presented, the proposal to allocate PACS modules on a divisional basis means that following a common mode failure of a single PACS module

type these safety systems will be vulnerable to a plant maintenance condition on one of the two remaining divisions. The reason for ignoring the plant maintenance condition is based on the requirements of the C&I safety principles document (Ref. 34) discussed above and for which no technical justification is provided. Allocating PACS modules according to whether the system provides a diverse means of achieving a safety function would avoid this problem. For example, EFWS and MHSI (through bleed and feed) provide a diverse means of achieving the decay heat removal function post-trip and so would be provided with diverse PACS module designs. In my opinion, there is a need for a future licensee to review the generic rule for the allocation of PACS modules using probabilistic techniques to ensure that it is optimum.

209 In contrast, the diversity implementation plan (Ref. 41) seems quite concerned about the possibility of a common mode failure of two PACS modules at 10^{-5} per demand causing the failure of a 1-out-of-1 single train on a safety system. Steamline isolation, MSRT isolation, and MSRT setpoint increase are highlighted for concern. I would have expected the probability of mechanical single failure to dominate the failure probability of a single train of such systems such that the common mode failure of PACS modules would be largely irrelevant.

210 It is noted that the discussion of loss of fuel pool cooling system faults in section 5.2 of the diversity plan (Ref. 41) appears to be out of date with the UK EPR™ design reference since this function has been upgraded to a Class 1 function and therefore needs to be allocated to the PS. It is also noted that the allocation of PACS modules to the support system actuators is still to be completed.

211 For all the above reasons, I have raised Assessment Finding **AF-UKEPR-FS-68** for a future licensee to review the PACS module allocation. In particular, I consider that PSA support is essential in ensuring that the number of lower order cut-sets is minimised particularly after taking account of plant maintenance states on systems associated with 2-out-of-4 success criteria.

212 A related matter is that during the assessment of the MHSI and LHSI systems which are claimed to be diverse systems on the UK EPR™ it became apparent that PACS modules are used to control four isolation valves on each of the four redundant trains that are common to both systems. Given that the valves are only closed to provide a containment isolation function for severe accident situations their normal default position is to be left open to ensure the safety injection function can be reliably performed without the possibility of an active single failure. EDF and AREVA argue that it is not physically possible for the PS to close these valves, it can only open them. Hence spurious operation of the PS cannot result in the valves closing. Spurious closure of the valves can potentially be caused by spurious operation of the SAS since it is intended that the operator should be able to close these valves manually using the SAS. However, in this case the PS can override the spurious operation since the PACS modules will give priority to the PS signal. Finally, EDF and AREVA claim that failure of a PACS module can only result in the failure of control function to occur and so the valve will be left in the open position upon common mode failure of the PACS modules. ONR would not agree with this claim but it is accepted that the PACS modules are of a simple design and the redundancy is four fold.

213 EDF and AREVA also note that regular flow tests will be performed during normal operation to check that the valves are in the correct position. This strategy has been assessed by an ONR C&I specialist who judge it to be acceptable (Ref. 11). Nevertheless, I want assurance that there are no other instances where the common mode failure of a single design of PACS module can potentially result in the failure of two

diverse systems both contributing to the same safety function. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-69** for a future licensee to review all valve and motor actuations to ensure that the design logic is such that common mode failure of a PACS module cannot result in the failure of two diverse systems both contributing to the same safety function. Consideration also needs to be given to common mode failure of the PS resulting in a spurious signal that overrides a correct signal from the SAS/NCSS.

4.13.3 Findings

214 I am content that sufficient progress has been made with the diversity implementation plan covering the allocation of PACS modules to justify the closure of Action 9 of GDA issue **GI-UKEPR-CI-06** from a fault studies perspective. My fundamental judgement is that two diverse designs of PACS modules should be sufficient to provide adequate diverse coverage for the plant actuators on the UK EPR™. However, I also believe that the precise distribution/allocation of PACS modules to individual plant actuators and C&I safety system platforms needs further optimisation to ensure that maximum benefit is made of the diverse designs. For these reasons, I have raised two Assessment Findings **AF-UKEPR-FS-68** and **AF-UKEPR-FS-69** on the application of PACS modules. While I have raised these Assessment Findings, I am confident that these will be resolvable during site specific detailed design phase and should not have any impact upon plant layout.

4.14 Assessment of the NCSS

4.14.1 Summary of EDF and AREVA's Safety Case

215 EDF and AREVA state that the safety function of the NCSS is to provide protection against the total loss of computerised C&I. Based on the requirements of the BSO of SAP T.9 for a summated risk of 10^{-7} per year, EDF and AREVA aim to protect against all design basis faults with a frequency greater than 10^{-3} per year, where they are assuming a individual sequence target of 10^{-9} per year and a conditional failure probability for the PS and SAS of 10^{-6} failures per demand. An additional requirement is that for initiating frequencies greater than 10^{-2} per year the NCSS is also to provide a further means of actuating the severe accident mitigation features. Finally, initiating faults that can be caused by the failure of computer based systems are to be protected by the NCSS assuming an initiating event frequency in coincidence with failure of both the PS and SAS of 10^{-6} per year. Again, the requirement is for the NCSS to also be able to initiate severe accident mitigation features.

216 The basis of the EDF and AREVA safety case is that they have reviewed each of these initiating faults and provided a functional analysis that the NCSS is capable of performing its role. In particular, for a selection of faults which they consider the most representative they have performed detailed transient analysis studies to demonstrate that the NCSS is able to detect the fault and initiate reactor trip and other engineered safeguard features sufficiently quickly to either prevent DNB or avoid significant fuel damage.

217 EDF and AREVA argue that on the basis of the analysis presented adequate justification has been provided on the functionality of the NCSS for the purposes of GDA, recognising that further design work will be performed during the site specific detailed design phase.

4.14.2 Assessment

218 During the close-out phase of GDA, EDF and AREVA have been requested to provide a technical justification for the functional specification of the NCSS through TQ-EPR-1567 (Ref.9) in support of the close-out of **GI-UKEPR-CI-01**. In response to the Technical Query, EDF and AREVA have provided the following documents:

- Functional Requirements on Non-computerised safety I&C functions (Ref. 42).
- Functional Justification of the NCSS Design (Ref. 43).
- Spurious opening of a Pressuriser Safety Relief Valve in case of loss of computerised I&C (Ref. 44).
- Comparison of the NCSS functions and SAS diversified functions (Ref. 45).

219 The functional requirements document (Ref. 42) provides the functional specification for the NCSS. This document provides a very clear definition of the functions that will be provided on the NCSS. The document notes that some of the more detailed requirements are still to be determined and so further work will be required during site specific detailed design phase. In particular, support systems are excluded from consideration. Given that the functional requirements document limits itself to listing the functions of the NCSS, the main safety justification for the NCSS is now provided in the supporting NCSS functional justification document (Ref. 43) which is the main document that I have assessed. The NCSS functional justification document outlines the design intent for the NCSS. It explains the methodology for determining the fault sequences for which it is expected to provide protection and provides supporting studies to demonstrate the functional capability of the design to protect against these sequences by selecting four representative sequences for transient analysis studies (loss of feed, excessive increase in steam flow, boron dilution, and loss of offsite power). These studies have been supplemented by an additional study looking at the small break loss of coolant accident at the request of ONR (Ref. 44). EDF and AREVA have also supplemented the studies (Ref. 45) by comparing the list of sensors on the NCSS with those provided on the Protection System (PS) and Safety Actuation System (SAS).

220 As noted above, the safety function of the NCSS is to provide protection against the total loss of computerised C&I. Based on the requirements of an individual sequence target of 1×10^{-9} per year EDF and AREVA intend that the NCSS should protect against all design basis faults with a frequency greater than 1×10^{-3} per year, where they are assuming a conditional failure probability for the PS and SAS of 1×10^{-6} failures per demand. An additional requirement is that for initiating frequencies greater than 1×10^{-2} per year the NCSS is also to provide for the actuation of severe accident mitigation features. Finally, initiating faults that can be caused by the failure of computer based systems are to be protected by the NCSS assuming an initiating event frequency in coincidence with failure of both the PS and SAS of 1×10^{-6} per year. Again, the requirement is also for the NCSS to be able to initiate severe accident mitigation features. Importantly, the initiating events for these sequences are based on the assumption that the computer based C&I system can only fail in two modes; the controller can freeze or go to zero. Spurious actuation is excluded from consideration. However, it must be recognised that in practice most spurious initiating events associated with C&I failures are in any case PCC-2 events. These are frequent faults and so this restriction on the failure modes has little effect in practice apart from one specific sequence (inadvertent closure of all four MSIVs) that is discussed further below.

221 Given the above assumptions, a list of initiating faults is developed for which the NCSS is intended to provide protection. I have reviewed this list against the list of design basis

events and it appears appropriate. The only fault missing that might be judged to be frequent is inadvertent closure of all four MSIVs which is discussed further below. However, the report notes that loss of support system faults associated with the closure of GDA issue **GI-UKEPR-FS-05** are not currently considered. An ONR PSA specialist (Ref. 12) has also reviewed the list of faults and considers it to be adequate for the purposes of GDA although noting that some frequent hazards and spurious C&I actuations are missing.

222 Although the list of faults is judged to be adequate for the purposes of GDA, it should be noted that not all the faults identified in the list as needing to be analysed have actually been assessed at this stage within the NCSS functional justification document. From a review of Table 2 of the report (Ref. 43), it is clear the following faults are not currently addressed:

- main feedwater malfunction resulting in a reduction in feedwater temperature;
- interfacing system LOCAs;
- loss of main grid for longer than 24 hours – shutdown state aspects;
- loss of main grid for longer than 24 hours – fuel pool aspects;
- small SGTR;
- stuck open Pressuriser Safety Valve (but note below);
- spurious withdrawal of one RCCA;
- loss of one train of fuel pool cooling system (state F);
- reactor draining via CVCS draining line (state E), and;
- voluntary draining of reactor with fuel pool connected (state D or F).

223 In addition, EDF and AREVA note that additional work (Ref. 42) will be required during the site specific detailed design phase to complete the functional design of the NCSS. This includes:

- Verification that all the reactor trips proposed to protect the plant for each postulated initiating event are relevant (especially regarding reactivity distribution transients).
- Design of the automatic thresholds.
- Definition of the response time and accuracy required for NCSS functions and conditions in which they are useful.
- Analyse the remaining accidents (especially SGTR, new postulated initiating events associated with the assessment of **GI-UKEPR-FS-05** on support systems, and fuel pool cooling accidents).
- Design of support systems actuators (including CCWS, HVAC, EDG).
- Analyse in detail the severe accident mitigation with the NCSS (required functions, time delay for their actuation).
- Analyse the procedural aspects to identify information needs for the MCR.

224 For this reason, I have raised Assessment Finding **AF-UKEPR-FS-70** for a future licensee to close out these items of work during the site specific detailed design phase.

225 The NCSS functional justification report (Ref. 43) then reviews each of the faults presented in Table 2. In Appendix A, a review of each fault is provided giving a qualitative

justification for why the NCSS provides adequate protection. Given that all the faults are frequent initiating events, those on the reactor generally involve intact circuit faults except for those associated with shutdown states. The strategy adopted therefore is to demonstrate an automatic reactor trip in the short term, with other longer term actions performed manually to simplify the NCSS design unless actuation of an engineered safety feature is required relatively quickly. The strategy also involves using bleed and feed as the preferred means of achieving long-term decay heat removal and reactivity control. However, to extend the timescale available for operator action prior to commencing bleed and feed operations, automatic actuation of the EFWS is provided to ensure short-term decay heat removal. Noticeably, no means (automatic or manual) is provided for actuation of the EBS. Since this would further extend the grace times available before the operator action is required to commence bleed and feed operations, I consider there is a case for at least providing for manual actuation of the EBS. For this reason, I have raised Assessment Finding **AF-UKEPR-FS-71** for a future licensee to explore the feasibility of providing manual actuation of the EBS function on the NCSS during the site specific detailed design phase.

226 Four faults are selected as representative of cooldown faults, heat-up faults, reactivity faults and loss of support system faults for more detailed transient analysis studies. A commitment is made for a more formal demonstration to be provided for the other faults during the site specific detailed design phase. I consider that this work is included in the scope of Assessment Finding **AF-UKEPR-FS-70** already discussed above. The selection of excessive increase in steam flow, loss of feed, homogeneous boron dilution and loss of off-site power appears appropriate for the purposes of GDA. In addition, I specifically requested that EDF and AREVA consider spurious opening of a PSV as representative of a decrease in reactor inventory fault (Ref. 44). As noted above, at this time no demonstration of the role of the NCSS in protecting against severe accident sequences is provided although part of the scope of the NCSS is to provide protection for such sequences for the most frequent initiating events.

227 The transient studies are performed on a best estimate basis. In practice, no single failure, plant maintenance state or consequential loss of off-site power is considered. Given the sequence frequencies, in my opinion these assumptions are reasonable. In addition, all thermal hydraulic parameters are assumed to have nominal values, as are thresholds, delays, and system characteristics. It is stated that the neutronic moderator feedback coefficients and decay heat are also nominal. My expectation is that for frequent faults being considered the safety margins will be sufficient such that, with the exception of the neutronic data, these uncertainties will not be too significant. However, for each transient, EDF and AREVA have helpfully provided an additional key parameter study in which penalised data is used and the claim on operator action is delayed for as long as possible. These studies are extremely useful and the approach is welcomed. The PCC-4 safety criteria are assumed for the safety limits.

228 One aspect of the NCSS design intent is that the computerised C&I (when available) should so far as is possible trigger the safeguard actions before the NCSS. The intent of EDF and AREVA is to achieve this by selecting the NCSS set points taking account the uncertainty associated with the C&I sensors and conditioning units. In my opinion the approach is appropriate and should not result in too penalising a delay for the NCSS actuation. However, EDF and AREVA are proposing some additional time delays for some functions and so the acceptability of these proposals can only be fully confirmed when all the studies listed above are complete. Confirmation of the selection of the set points is an issue that in my opinion can be left until the site specific detailed design phase.

229 The first fault analysed in Appendix C (Ref. 43) is the excessive increase of steam flow fault due to spurious opening of an MSRT. The transient analysis only considers the post-trip avoidance of return to criticality arguing that the work performed for functional diversity for frequent faults under Action 2 of GDA issue **GI-UKEPR-FS-02** discussed above demonstrates adequate margin for a reactor trip based on SG level trip. Given that all the RCCAs are assumed to insert, the accumulators automatically inject borated water, and the main feedwater system is automatically isolated by the NCSS on low SG level, the studies demonstrate considerable shutdown margin even assuming penalised moderator feedback coefficients. However, as part of the work performed in closing out Action 2 of GDA issue **GI-UKEPR-FS-02** discussed in Section 4.2.1 above, the claim on SG level trip and actuation has been undermined because there is potential for the feed controller to adversely affect this parameter. EDF and AREVA are now looking to explore using the neutron flux detectors as a diverse trip parameter for this fault. This issue is already covered by Assessment Finding **AF-UKEPR-FS-41** for a demonstration of the effectiveness of the ex-core flux detectors to protect against this fault to be provided during the site specific detailed design phase (for both the SAS and the NCSS). However, as noted above, my judgement is that the ex-core detectors should be efficient at protecting against this fault and I note that the current design of the NCSS already includes an automatic reactor trip on high flux. I therefore judge that the GDA issue **GI-UKEPR-CI-01** covering the functional specification for the NCSS can be closed with regard to this frequent fault.

230 The second fault analysed in Appendix D (Ref. 43) is the loss of main feedwater fault. The NCSS trips the reactor on low SG level and automatically actuates the EFWS. The automatic actuation of the EFWS provides considerable margin to any safety limits even for the penalised studies using conservative decay heat levels.

231 The third fault analysed in Appendix E (Ref. 43) is the loss of off-site power. Since the assumed failure of the computerised C&I also results in the failure of the EDGs to start the fault effectively becomes a station blackout sequence for which EFWS will not be available despite an automatic actuation being available on the NCSS. Loss of cooling to the RCP seals is assumed to result in a small loss of coolant break at each RCP. The reactor is tripped on high hot leg pressure or low pressure drop across the RCP by the NCSS. The operator is claimed to manually start the EDGs and perform a bleed and feed operation using the NCSS to actuate the MHSI and LHSI pumps and to open a PDS valve. The NCSS also provides the pressure vessel level indication to inform the operator when to perform the bleed and feed operation. As well as a best estimate calculation, sensitivity studies are performed on the maximum time available for operator action and assuming penalised decay heat levels. The studies demonstrate that the switch to conservative decay heat data does not significantly alter the timing of the transient. The best estimate analysis assumes the operator performs the bleed and feed operation at 3759 seconds. The first sensitivity study demonstrates that this can be delayed until 4628 seconds. The analysis associated with conservative decay heat data reduces the estimated time available to 4268 seconds.

232 However, the claim on starting the EDGs made in the above analysis appears questionable since, as noted in Section 4.8.2 above, the emergency operating procedures have been updated to drive the operator to start the UDGs in preference to the EDGs to improve the reliability of the operator actions given the short timescales. If this is also the case for LOOP with loss of PS/SAS, this might have an impact on the transient studies since with the current allocation of electrical loads (Ref. 46) only two LHSI trains are available to provide safety injection using the UDGs rather than the four MHSI/LHSI trains that are assumed in the analysis. The issue of electrical loading is being addressed by

EDF and AREVA in the response to GDA issue **GI-UKEPR-FS-05** (Ref. 27) covering loss of support systems including the electrical system, which is looking to optimise the allocation of electrical loads and which should ultimately ensure that an adequate number of SIS trains will be available. This does not necessarily alter the conclusions of the study that the NCSS has in principle adequate functionality to protect against this fault but this will need to be confirmed. In particular, there may be a case for providing for the manual actuation of either the EDGs or the UDGs from the NCSS. I have therefore raised Assessment Finding **AF-UKEPR-FS-72** for a future licensee to provide justification for the claim on the EDGs or to provide an alternate justification for this particular sequence.

233 It should also be noted that the stand-still seal system is also potentially available to protect against the possibility of a LOCA following loss of cooling to the RCP seals. I have therefore raised Assessment Finding **AF-UKEPR-FS-73** for a future licensee to consider the feasibility of providing the capability for manually actuating the stand-still seal system on the NCSS.

234 The fourth fault analysed in Appendix F (Ref. 43) is the malfunction of the CVCS causing a decrease in boron concentration during shutdown operation. The studies claim the operator to manually isolate the CVCS using the NCSS as a precaution following loss of computer based C&I so as to provide protection against a potential dilution fault. The transient analysis studies are used to demonstrate that adequate time is available to isolate such a fault before return to criticality occurs. Depending on the initial RCS conditions the time scales vary from one to two hours. The penalised studies have only a minor effect on the transient times.

235 The additional fault analysed (Ref. 44) is the spurious opening of a pressuriser safety valve fault. The studies claim the NCSS to trip the reactor on low hot leg pressure, the RCPs on low pressure drop, and isolate the CVCS on low pressuriser pressure. The operator is then expected to start the MHSI pumps and commence bleed and feed operations using the PDS valves. Again sensitivity studies are performed for the operator action time and to key parameters such as decay heat levels. The studies confirm that the switch to conservative decay heat data does not significantly alter the timing of the transient. The best estimate analysis assumes the operator performs the bleed and feed operation at 2199 seconds. The first sensitivity study shows that this can be delayed until 2826 seconds. The analysis associated with conservative decay heat data reduces the estimated time available to 2576 seconds.

236 As noted above, there is one additional sequence that I would have liked EDF and AREVA to consider and this is the spurious closure of all four MSIV with failure of the computer based C&I since this is a very rapid transient. Based upon the analysis performed for frequent faults during GDA, my judgement is that the high hot leg pressure trip on the NCSS together with the lifting on the MSSVs and PSVs should provide adequate protection for this fault but I would like to see this confirmed during the site specific detailed design phase. I have therefore raised Assessment Finding **AF-UKEPR-FS-74** for a future licensee to provide such a study.

237 As an independent check, EDF and AREVA were requested to provide a comparison of NCSS functions against the diversified SAS and PS (Ref. 45). The study generally demonstrates reasonable coverage by the NCSS. The main difference is that a lot of the engineered safeguard features are operated manually on the NCSS. The NCSS also relies upon bleed and feed using the PDS valves rather than partial cooldown to lower RCS pressure to enable safety injection since the MSRT opening set point cannot be reduced by the NCSS. The report acknowledges that the SGTR transient has still to be analysed. Although the NCSS has slightly more limited functionality, given the sequence

frequencies being considered the approach is judged to be appropriate subject to confirmation during the site specific detailed design phase. As part of Assessment Finding **AF-UKEPR-FS-62,** a future licensee is expected to provide such a justification.

4.14.3 Findings

238 Overall, I am content that the functional specification for the NCSS presented in the supporting documentation submitted in response TQ-EPR-1567 is sufficient for the closure of GDA issue **GI-UKEPR-CI-01** from a fault study perspective. My fundamental judgement in reaching this conclusion is that the NCSS is essentially performing a similar role to that of the SAS in protecting against failures on the PS. The SAS has already been analysed against the failure of the PS for frequent faults and spurious actuation signals. Therefore, if it is assumed that the SAS were to fail in its role, the most onerous implications for the NCSS design would be that it needs to provide the same functionality as the SAS. Given that the same sensors and actuators used for the SAS are potentially available for the NCSS, it is unlikely that any future increase in the scope of the NCSS required during the site specific detailed design phase will have any implications on plant layout. I am therefore satisfied that GDA issue **GI-UKEPR-CI-01** can now be closed.

239 I have raised Assessment Findings **AF-UKEPR-FS-70** to **AF-UKEPR-FS-74**. These are items generally requiring further confirmatory work or limited changes in the functionality of the NCSS. My judgement is that they are unlikely to result to changes in plant layout.

4.15 Classification of the CVCS and Diverse Safety Injection

4.15.1 Summary of EDF and AREVA's Safety Case

240 The CVCS is an auxiliary fluid system that supports the continued satisfactory performance of the reactor coolant system during all operating conditions including at power operation, shutdown and start-up. It ensures that the fuel is maintained in an appropriate environment by controlling the inventory and chemistry of the primary circuit and in conjunction with the RCCAs ensures adequate reactivity shutdown and hold-down capability under all operating conditions. Its main safety functions are:

- To maintain the primary coolant inventory.
- To control the chemical purity, activity, hydrogen, pH and boron concentrations of the primary coolant.
- To provide seal water injection flow to the seals of the RCPs during normal and fault conditions.
- To provide a capability for RCS boration and make-up.
- To provide an emergency letdown route.

241 The CVCS consists of several sub-systems including the charging, letdown and seal water system, and the reactor coolant and purification and chemistry control system.

242 EDF and AREVA have performed a functional analysis of the CVCS and concluded that apart from a number of isolation functions, the main safety functions of the CVCS (charging, letdown, seal water) should be given a safety classification of Class 3.

4.15.2 Assessment

243 In response to the GDA issue **GI-UKEPR-CC-01**, EDF and AREVA have applied their categorisation and classification methodology (Ref. 47) developed during GDA to the

categorisation and classification of the CVCS (Refs 47 and 48) with additional information provided in their response to TQ-EPR-1615 (Ref. 9). Using this methodology, EDF and AREVA have identified 24 safety feature groups on the CVCS. The seven mechanical safety features associated with the isolations due to the interface of the CVCS with either the containment building or the primary pressure circuit are allocated Class 1 as expected. One safety feature is associated with isolations to protect against boron dilution faults and is also classified as Class 1. All remaining safety features are classified as Class 3 apart from the control function on the letdown flow which is Class 2. This appears to contrast markedly with the classification of the CVCS on Sizewell B which is mostly classified at the equivalent of Class 1 although it is recognised that the equivalent of a Class 2 designation does not exist on Sizewell B and so anything that would be the equivalent of a Class 2 has of necessity to be Class 1.

244 It should be noted that the design intent for the CVCS on the UK EPR™ is different from that of the CVCS on Sizewell B. On Sizewell B the CVCS is designed as a safety system to perform a diverse safety injection role. This is because the valves in the suction lines to the HHSI and LHSI pumps on Sizewell B consisting of two non-return valves and motorised valve are common and therefore the safety case acknowledges that no diversity can be claimed between them. In addition, there is also only a single line through the containment wall between the refuelling water storage tank and the common header of the safety injection systems. For these reasons, following common mode failure of the MHSI and LHSI in response to a frequent small break LOCA the operator is expected to depressurise the primary circuit and re-instate CVCS make-up. The lower primary circuit pressure increases the make-up capacity of the CVCS and reduces the rate of coolant loss through the break such that the CVCS has sufficient capacity to ensure adequate cooling of the fuel.

245 In contrast, EDF and AREVA claim that the MHSI and LHSI systems on the UK EPR™ are diverse systems. To better understand this claim, I raised TQ-EPR-1630 (Ref. 9). Subsequently, EDF and AREVA supplemented this response with further information (Ref. 49). EDF and AREVA argue that the IRWST is located inside containment eliminating the need for a single pipe to pass through containment. This enables each of the four redundant SIS trains to take its suction from one of four redundant lines on the IRWST. However, there is still a single valve on each suction line that is shared between the MHSI and the LHSI trains for that line. These are the valves that are discussed in the assessment of PACS module diversity in Section 4.12.2 above. Essentially, EDF and AREVA are arguing (Ref. 49) that the valves are passive features since they should already be open and therefore do not need to be realigned during a fault. They argue that the pumps are tested every 4 months while the reactor is at power to ensure that these valves are correctly aligned to eliminate human error closing them during an outage. Incorrect positioning of the valves is also alarmed. On this basis, no common cause cut-off frequency is modelled in the PSA for failure of these valves. As discussed above, ONR does not agree with this practice although it is accepted that the common mode failure rate for the PACS modules is quite low.

246 Each MHSI and LHSI train also shares a non-return valve on the cold leg injection line. However, EDF and AREVA in their response to TQ-EPR-1515 (Ref. 9) note that the operator can manually open the hot leg injection lines to provide a diverse means of LHSI injection. While my judgement is that this is probably an acceptable argument no formal justification has been provided within the diversity review to demonstrate this claim including transient analysis studies and a human factors assessment to demonstrate that the procedure could be reliably performed. For this reason, I have raised Assessment

Finding **AF-UKEPR-FS-75** for a future licensee to demonstrate that hot leg injection provides an adequate diverse means of safety injection for frequent SBLOCA faults.

247 Since EDF and AREVA claim that the MHSI and LHSI systems are diverse, the CVCS is designed to perform only a prevention function rather than a protection function for which classification at Class 3 is appropriate, although still recognising it has a significant risk reduction role. In their response to TQ-EPR-1530 (Ref. 9), EDF and AREVA argue that upgrading the system to Class 2 requirements would require a significant number of changes to electrical switchboard allocation, C&I allocation, support systems allocation including a change in the CCWS header from which the charging pumps take their cooling. A number of isolation signals would also need to be reviewed. EDF and AREVA are also concerned that in the situation where the MHSI has failed and the operator is expected to commence a fast cooldown to allow LHSI to start injection he may be confused and start the CVCS, which depending on the break size may not have sufficient capacity to cope with the fault. The response to TQ-EPR-1515 (Ref. 9) also notes that the CVCS is not designed for conditions where the RCS inventory is contaminated due to damage to the fuel cladding arising from the fault. For this reason, EDF and AREVA have raised CMF#33 (Ref. 8), which provides an automatic Class 1 isolation of the CVCS letdown based upon high activity in the primary circuit. Furthermore, in contrast with Sizewell B, the CVCS regenerative heat exchanger is located inside containment and so its pressure boundary is not to be designed to nuclear standards although I recognise that this is consistent with Class 3 requirements.

248 In their response to TQ-EPR-1515 (Ref. 9), EDF and AREVA state that the reliability claim of the CVCS make-up function is 2×10^{-3} with an associated risk increase factor of 1.01. My judgement is that the risk increase factor would increase when a more realistic common mode failure frequency is included for the spurious failure of the PACS. Hence it should be recognised that the reliability requirements on the CVCS put it on the margins of the classification boundary between Class 2 and Class 3 systems. Although my preference would have been for the charging, letdown and seal water systems to have been classified as Class 2, I judge that it would be disproportionate to expect EDF and AREVA to upgrade the system from Class 3. Nevertheless, given the reliability claims in the PSA it may be appropriate and ALARP for the availability of the CVCS to be controlled through the technical specifications and for the examination, inspection, maintenance and testing regime applied to the CVCS to be enhanced to Class 2 standards.

249 Chapter 18.2 of the PCSR (Ref. 22) states that maintenance of F2 systems (the equivalent of Class 3 system in the UK EPR™ classification methodology) may be authorised in general at any time. It is also proposed that for equipment that is considered to be non-critical, preventive maintenance will be limited to minor operations such as upkeep and lubrication essential for smooth running. EDF and AREVA argue that on such equipment, it is legitimate to wait for a failure to occur before intervening. For this reason, Assessment Finding **AF-UKEPR-FS-76** has been raised for a future licensee to present its proposed maintenance arrangements for Class 3 duty systems such as the CVCS and to confirm such systems will still be included on the maintenance schedule with requirements for periodic maintenance or appropriate condition monitoring.

250 This discussion illustrates a difficulty with the classification methodology of EDF and AREVA as the boundary between a diverse function (associated with Category A but system Class 2) and a risk reduction function (associated with Category C and system Class 3) is open to interpretation. This difficulty can only be overcome in practice by gaining confidence in how a future licensee applies the methodology to the UK EPR™. For this reason, ONR may wish to assess the response that a future licensee makes to

cross-cutting Assessment Finding **AF-UKEPR-CC-05** requiring the application of the classification process to the UK EPR™ in some detail.

4.15.3 Findings

251 Following my assessment of the classification of the CVCS, I have raised two Assessment Findings. **AF-UKEPR-FS-75** is for a future licensee to demonstrate that hot leg injection provides an adequate diverse means of safety injection for frequent SBLOCA faults while **AF-UKEPR-FS-76** is for a future licensee to present its proposed maintenance arrangements for Class 3 duty systems such as the CVCS and to confirm they will still be included on the maintenance schedule covering periodic maintenance or appropriate condition monitoring.

5 ASSESSMENT CONCLUSIONS

252 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-02** (and the related GDA issues under **GI-UKEPR-CC-01**, **GI-UKEPR-CI-01** and **GI-UKEPR-CI-06**) to improve the demonstration of functional diversity for frequent faults identified in my GDA Step 4 assessment report.

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

- Addition of a high hot leg pressure trip signal on the Safety Actuation System (SAS) to improve the protection against loss of normal feedwater faults occurring together with a failure of the main reactor protection system.
- Addition of a low Reactor Coolant Pump (RCP) speed trip signal on the SAS to improve the protection against reduction in flow faults occurring together with a failure of the main reactor protection system.
- Addition of a high neutron flux trip signal and a high axial offset trip signal on the SAS to improve the protection against reactivity faults occurring together with a failure of the main reactor protection system.
- Implementation of a diverse protection function to mitigate homogeneous boron dilution faults in shutdown conditions occurring together with a failure of the main reactor protection system. The options identified for further study include provision of a diverse source range detector on the SAS or provision of a diverse boron meter on the SAS to be located on either a Nuclear Sampling System (NSS) line or the Chemical Volume and Control System (CVCS) charging or letdown line together with associated automatic protection actions.
- Upgrade to Class 2 of the actuation signal used for manually starting the Ultimate Diesel Generators (UDG).
- Upgrade to Class 2 of the actuation signal used for manually opening the Primary Depressurisation System (PDS).
- Upgrade to Class 2 of the actuation signal used for automatically closing the diverse full load Main Feedwater Isolation Valves.
- Upgrade to Class 2 of the Anticipated Trip without Scram (ATWS) signal used for the automatic actuation of the Emergency Boration System (EBS).
- Upgrade to Class 2 of the automatic CVCS charging pump switchover.
- Upgrade to Class 2 of the automatic diverse CVCS anti-dilution isolation.
- Upgrade to Class 2 of the manual start-up of the diverse third Fuel Pool Cooling System (FPCS) train.
- Upgrade to Class 2 of the (FPCS) purification pump trip.

254 Although there are a large number of Assessment Findings, these are mostly associated with the C&I protection systems. In my judgement, it is unlikely that any design changes identified as a result of the closure of these Assessment Findings will result in significant changes to plant layout.

5.1 Overall Conclusions

255 Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that the demonstration of functional diversity for frequent faults on the UK EPR™ presented in the supporting documentation submitted in response to GDA Issue **GI-UKEPR-FS-02** is adequate 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-02** can now be closed.

6 ASSESSMENT FINDINGS

6.1 Additional Assessment Findings

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

AF-UKEPR-FS-41: *The future licensee shall demonstrate that the ex-core neutron flux detectors are functionally capable of providing diverse protection against excessive increase in secondary steam flow faults including spurious lifting of the Main Steam Relief Train (MSRT) valves so as to avoid Departure from Nucleate Boiling (DNB).*

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

AF-UKEPR-FS-42: *The future licensee shall demonstrate that the in-core Self-Powered Neutron Detectors (SPND) are functionally capable of protecting against Rod Cluster Control Assembly (RCCA) misalignment faults including one or more dropped RCCAs and against uncontrolled single RCCA withdrawal faults assuming the loss of the most onerous SPND finger due to a single failure such that DNB is avoided using conservative PCC analysis rules and conservative methods and assumptions.*

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

AF-UKEPR-FS-43: *The future licensee shall explore the feasibility of using the axial offset signal derived from the ex-core detectors as a diverse means of ensuring the reactor is sufficiently well trimmed so as to avoid entering DNB following RCCA misplacement faults including the dropping of more than one RCCA together with common mode failure of the SPNDs.*

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

AF-UKEPR-FS-44: *The future licensee shall determine which of the options identified within Change Management Form (CMF) #59 is to be developed into fully worked up proposal to provide diverse protection against homogeneous boron dilution faults occurring during shutdown conditions.*

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

AF-UKEPR-FS-45: *The future licensee shall perform a functional diversity analysis for all frequent faults considering the common mode failure of each of the essential support systems to demonstrate that adequate functional diversity is provided.*

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

AF-UKEPR-FS-46: *The future licensee shall provide a fully integrated safety case for the station blackout sequence.*

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

AF-UKEPR-FS-47: *The future licensee shall review the definition of the controlled state against the definition of the non-hazardous stable state to ensure that the categorisation of reactivity control function (and classification of associated systems responsible for RCS boration) is appropriate.*

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

AF-UKEPR-FS-48: *The future licensee shall perform an ALARP assessment on the feasibility of providing a diverse means of isolating one pair of steam lines from the other pair following a break on the secondary side.*

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

AF-UKEPR-FS-49: *The future licensee shall demonstrate diverse protection for frequent cold overpressure faults.*

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

AF-UKEPR-FS-50: *The future licensee shall review the demonstration of functional diversity for frequent faults to ensure it is applicable for all plant states.*

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

AF-UKEPR-FS-51: *The future licensee shall perform an ALARP assessment on the feasibility of tripping the main feedwater pumps as a diverse means of ensuring feedwater isolation.*

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

AF-UKEPR-FS-52: *The future licensee shall review the implications of assuming plant maintenance states on the demonstration of functional diversity for frequent initiating events unless it can be shown that the sequence frequency is below 10^{-7} per year.*

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

AF-UKEPR-FS-53: *The future licensee shall update the PCSR to reflect the definition of controlled state for fuel pool faults, the functioning of the RCSL anti-dilution safety function, the change in protection claimed for excessive increase in secondary steam flow faults with failure of PS and the inclusion of support system functions in the fault and protection schedule.*

Required timescale: *Fuel on Site*

AF-UKEPR-FS-54: *The future licensee shall complete the work on demonstration of functional diversity for sensors and conditioning modules by including consideration of support system faults, spent fuel pool faults, frequent internal and external hazards, boron dilution faults and the revised safety case for excessive increase in secondary steam flow faults.*

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

AF-UKEPR-FS-55: *The future licensee shall consider the feasibility of providing a diverse reactor trip and safety injection signal on the SAS based upon a high containment pressure signal.*

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

AF-UKEPR-FS-56: *The future licensee shall consider the feasibility of providing a diverse reactor trip and safety injection signal on the SAS based upon detection of the existing low cold leg temperature signal.*

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

AF-UKEPR-FS-57: *The future licensee shall provide justification for not providing a diverse reactor trip signal on the SAS based upon detection of turbine trip signal.*

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

AF-UKEPR-FS-58: *The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of low RCP current.*

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

AF-UKEPR-FS-59: *The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of low RCP voltage.*

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

AF-UKEPR-FS-60: *The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of the existing low SG pressure signal.*

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

AF-UKEPR-FS-61: *The future licensee shall develop a PSA model of the UK EPRTM C&I systems to adequately assess the impact on risk of the allocation of sensors, conditioning modules and PACS modules, especially in terms of dependency.*

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

AF-UKEPR-FS-62: *The future licensee shall provide justification for those functions on the SAS and NCSS for which reliance will be placed upon manual actuations.*

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

AF-UKEPR-FS-63: *The future licensee shall provide transient analysis studies to demonstrate that there is adequate diverse protection against the loss of one RCP.*

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

AF-UKEPR-FS-64: *The future licensee shall provide transient analysis studies to demonstrate that there is adequate diverse protection against the uncontrolled single RCCA withdrawal fault.*

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

AF-UKEPR-FS-65: *The future licensee shall review the allocation of conditioning modules for the in-core and ex-core detectors to reduce the risk to ALARP of both systems being unavailable following common failure of a single design of conditioning module.*

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

AF-UKEPR-FS-66: *The future licensee shall perform a review of the allocation of conditioning modules using the PSA model developed under AF-UKEPR-FS-61 taking into account plant maintenance states and provide a technical justification for excluding consideration of the most onerous plant maintenance state within the safety principles applied to the UK EPRTM C&I architecture.*

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

AF-UKEPR-FS-67: *The future licensee shall review and update the C&I safety features classification document to ensure diverse C&I systems are appropriately classified.*

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

AF-UKEPR-FS-68: *The future licensee shall perform a review of the allocation of PACS modules using the PSA model developed under AF-UKEPR-FS-61 taking into account plant maintenance states.*

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

AF-UKEPR-FS-69: *The future licensee shall review all valve and motor actuations to ensure that the design logic is such that common mode failure of a PACS module cannot result in the failure of two diverse systems both contributing to the same safety function. Consideration also needs to be given to common mode failure of the PS resulting in a spurious signal that overrides a correct signal from the SAS/NCSS.*

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

AF-UKEPR-FS-70: *The future licensee shall complete the analysis work required to fully define the functional specification of the Non-Computer based Safety System (NCSS). This includes verification of effectiveness of the claimed reactor trip signals, design of automatic thresholds, definition of response time together with required accuracy, remaining faults including SGTR, support systems, and fuel pool faults, design of support system*

actuators, analyses of severe accident mitigation, and information needs in MCR.

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

***AF-UKEPR-FS-71:** The future licensee shall consider the feasibility of providing a manual actuation function on the NCSS of the Emergency Boration System (EBS).*

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

***AF-UKEPR-FS-72:** The future licensee shall clarify whether reference to the Emergency Diesel Generators (EDG) made in the justification of the functional specification for the NCSS for the case of loss of off-site power is correct or provide an alternate justification for this fault sequence.*

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

***AF-UKEPR-FS-73:** The future licensee shall consider the feasibility for providing the capability for manually actuating the stand-still seal system on the NCSS.*

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

***AF-UKEPR-FS-74:** The future licensee shall confirm that the high hot leg pressure signal on the NCSS is functionally capable of providing protection against the spurious closure of all four MSIVs with failure of the computer based C&I systems.*

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

***AF-UKEPR-FS-75:** The future licensee shall demonstrate that hot leg injection provides an adequate diverse means of safety injection for frequent SBLOCA faults.*

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

***AF-UKEPR-FS-76:** The future licensee shall present its proposed maintenance arrangements for Class 3 duty systems such as the CVCS.*

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

257 These Assessment Findings are listed in Annex 2.

6.1.1 Impacted Step 4 Assessment Findings

258 As noted in the main text of the report, three 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. In addition, Assessment Finding **AF-UKEPR-FS-15** requires that transient analysis be performed to determine the LCOs for uncontrolled RCCA bank withdrawal at power faults together with failure of the PS to

avoid DNB and therefore presupposes that some of the modifications proposed under CMF#23 will be implemented. Similarly, **AF-UKEPR-FS-29** requires that the fault schedule in the PCSR is regularly updated to reflect revisions in the safety case.

259 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 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-02 Revision 2. Diversity for Frequent Faults.* ONR. July 2011. TRIM Ref. 2011/385302.

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-02 Revision 0.* EDF and AREVA. June 2011. TRIM Ref. 2011/347623.

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 15. UK EPR. December 2012. TRIM Ref. 2012/478281.

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

10 *C&I Assessment Report for Closure of GDA,* ONR Assessment Report ONR-GDA-AR-12-022 Revision 0 TRIM Ref. 2012/22

11 *C&I response to TQ-EPR-1630,* Letter EPR01403N, ONR Assessment Note, December 2012, TRIM Ref. 2012/488959

12 *Review of the adequacy from the PSA point of view of the NCSS "safety frame".* ONR Assessment Note, October 2012, TRIM Ref. 2012/339247.

13 *Human Factors Assessment Report for GI-UKEPR-HF-01,* ONR Assessment Report ONR-GDA-AR-12-009 Revision 0. TRIM Ref. 2012/09

14 *Excessive increase in steam flow – sensitivity analyses,* PEPR-F DC 84 Rev A, EDF and AREVA, December 2011, TRIM Ref. 2011/653104

15 *ATWS by loss of TXS – RCCA misalignment up to Rod drop,* Pepr.f.11.1467 Rev A, EDF and AREVA, December 2011, TRIM Ref. 2011/641790

16 *Demonstrate the provision of diverse protection against loss of CVCS following reactor trip and xenon decay including demonstration of diversity to operator action,* PEPR-F 11.0956, EDF and AREVA, July 2011, TRIM Ref. 2011/401857

17 *Development of a diverse protection system for CVCS homogeneous boron dilution events in shutdown states,* PEPCF.12.0678 Rev 1, EDF and AREVA, July 2012, TRIM Ref. 2012/280890

18 *Response to GI-UKEPR-FS-02 Actions 8 & 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

19 *Diversity for Frequent Faults: ATWS LOOP cumulated with automatic EDG start-up failure,* ECESN120274 Rev A, EDF and AREVA, May 2012, TRIM Ref. 2012/225086

20 *Diverse protection for the frequent faults involving the loss of essential support systems – Loss of off-site power with station blackout event,* Detailed in Letter EPR01386N, EDF and AREVA, September 2012, TRIM Ref. 2012/381285

21 *PCSR Sub-Chapter 14.7 – Fault and Protection Schedule*
UKEPR-0002-149 Issue 03, November 2012, TRIM Ref. 2012/472435
PCSR Sub-Chapter 16.5 – Adequacy of the UK EPR design regarding functional diversity
UKEPR-0002-167 Issue 01, November 2012, TRIM Ref. 2012/472450

22 *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 Submission Master List. November 2009. TRIM Ref. 2011/46364.

23 *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.

24 *Design Change Procedure,* UKEPR-I-003, Revision 11, EDF and AREVA, December 2012, TRIM Ref. 2012/478287.

25 *Response to TQ-EPR-1593,* PEPRF 12.1220 Rev 1, EDF and AREVA, September 2012, TRIM Ref. 2012/353312.

26 *Response to TQ-EPR-1539 related to loss of CVCS faults,* PEPR-F 12.0139, EDF and AREVA, January 2012, TRIM Ref. 2012/89195

27 *Fault Studies Assessment Report for GI-UKEPR-FS-05,* ONR Assessment Report ONR-GDA-AR-12-013 Revision 0. TRIM Ref. 2012/13

28 *Fukushima Lessons Learnt Assessment Report for GI-UKEPR-CC-03,* ONR Assessment Report, ONR-GDA-AR-12-025 Revision 0. TRIM Ref. 2012/25

29 *Closure of GI-UKEPR-FS-02 – Assessment of Claims for SBO DG Manual Start-up,* ONR Human Factors Assessment Note. TRIM Ref. 2012/483323

30 *Fault Studies Assessment Report for GI-UKEPR-FS-04,* ONR Assessment Report ONR-GDA-AR-12-008 Revision 0. TRIM Ref. 2012/8

31 *UK EPR – Main Steam Isolation Valves ALARP Assessment regarding functional diversity and Single Failure Criterion,* PESS-F DC 27 Rev A, EDF and AREVA, October 2012, TRIM Ref. 2011/93037

32 *Minutes of the 10th UK EPR™ Design Safety Review Committee – 8th February 2012,* EDF and AREVA, Detailed in letter EPR01140R, May 2012, TRIM Ref. 2012/190457

33 *Diversity implementation plan for sensors and conditioning,* PELA-F DC 3 Rev C, EDF and AREVA, October 2012, TRIM Ref. 2012/425767

34 *Safety principles applied to UK EPR™ I&C Architecture in terms of the requirements for diversity and independence,* PEPS-F DC 90 Rev C, EDF and AREVA, August 2012, TRIM Ref. 2012/342262

35 *Allocation of sensors and conditioning when three lines of defence are involved,* PEPS-F DC 148 Rev A, EDF and AREVA, October 2012, TRIM Ref. 2012/411783

36 *Diversity criteria for sensors and conditioning,* PELL-F DC 82 Rev C, EDF and AREVA, October 2012, TRIM Ref. 2012/424886

37 *Functional Analysis for sensors common cause failure,* PEPR-F DC 83 Rev C, EDF and AREVA, October 2012, TRIM Ref. 2012/425768

38 *UK EPR™ – Generic Design Assessment – Classification of I&C safety features,* ECEF091489 Rev E, EDF and AREVA, October 2012, TRIM Ref. 2012/417591

39 *Answer to TQ-EPR-1578 (sensor diversity),* PEPRF.12.0855, EDF and AREVA, June 2012, TRIM Ref. 2012/248030

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

41 *Diversity implementation plan for PACS Modules,* ECESN120472 Rev A, EDF and AREVA, July 2012, TRIM Ref. 2012/319795

42 *Function requirements on Non Computerised safety I&C functions,* NEPR-F DC 551 Rev C, EDF and AREVA, July 2012, TRIM Ref. 2012/284449

43 *Functional justification of the Non Computerised Safety System design,* PEPR-F DC 105 Issue A, EDF and AREVA, July 2012, TRIM Ref. 2012/284451

44 *Spurious opening of a Pressuriser Safety Valve in case of loss of computerised I&C (Response to TQ-EPR-1567),* PEPRF12.0966, EDF and AREVA, July 2012, TRIM Ref. 2012/284941

45 *Comparison of the NCSS functions and SAS diversified functions (Response to TQ-EPR-1567),* PEPRF12.1062, Rev 1, EDF and AREVA, August 2012, TRIM Ref. 2012/343682

46 *UK EPR GDA Electrical System CAE Document – 17074-709-000-RPT-0002* – Issue 05 October 2012 TRIM Ref. 2012/306714

47 *Methodology for Classification of Structures, Systems, Safety Features and Component,* NEPS-F DC 557, EDF and AREVA, October 2012, TRIM Ref. 2012/424300

48 *Classification of CVCS,* Detailed in Letter EPR01157R, EDF and AREVA, May 2012, TRIM Ref. 2012/202850

49 *Supplemental Response to TQ-EPR-1630,* Detailed in Letter EPR01403N, EDF and AREVA, October 2012, TRIM Ref. 2012/395945

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Topic	Document Ref.	Title	Ref.
GI-UKEPR-FS-02.A1	Loss of normal feedwater faults	CMF-23	Additional reactor trips on SAS C&I system	8
GI-UKEPR-FS-02.A2	Excessive increase in steam flow faults	PEPR-F DC 84 Rev A	Excessive increase in steam flow – sensitivity analyses	14
GI-UKEPR-FS-02.A2	Excessive increase in steam flow faults	PEPRF 12.1220 Rev 1	Response to TQ-EPR-1593	25
GI-UKEPR-FS-02.A3	Reduction in RCS flow faults	CMF-23	See Action 1	8
GI-UKEPR-FS-02.A4	Uncontrolled RCCA bank withdrawal faults	CMF-23	See Action 1	8
GI-UKEPR-FS-02.A5	Rod misplacement faults	PEPCF.11.1467 Rev A	ATWS by loss of TXS – RCCA misalignment up to Rod drop	15
GI-UKEPR-FS-02.A6	Loss of CVCS faults	PEPR-F 11.0956	Demonstrate the provision of diverse protection against loss of CVCS following reactor trip and xenon decay including demonstration of diversity to operator action.	16
GI-UKEPR-FS-02.A6	Loss of CVCS faults	PEPR-F 12.0139	Response to TQ-EPR-1539 related to loss of CVCS faults	26
GI-UKEPR-FS-02.A7	Homogeneous boron dilution faults	PEPCF.12.0678 Rev 1	Development of a diverse protection system for CVCS homogeneous boron dilution events in shutdown states.	17
GI-UKEPR-FS-02.A7	Homogeneous boron dilution faults	CMF-59	Diverse protection function for CVCS homogeneous boron dilution events in shutdown states.	8

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Topic	Document Ref.	Title	Ref.
GI-UKEPR-FS-02.A8	Loss of support system faults	Letter EPR01281N	Response to GI-UKEPR-FS-02 Actions 8 & 9 – Diversity for frequent faults and to GI-UKEPR-FS-05 Action 1 – Loss of support systems	18
GI-UKEPR-FS-02.A8	Loss of support system faults	ECESN120274 Rev A	Diversity for Frequent Faults: ATWS LOOP cumulated with automatic EDG start-up failure.	19
GI-UKEPR-FS-02.A8	Loss of support system faults	Letter EPR01386N	Diverse protection for the frequent faults involving the loss of essential support systems – Loss of off-site power with station blackout event.	20
GI-UKEPR-FS-02.A9	Diversity until safe shutdown state	NEPR-F DC 580 Rev B	Functional diversity for frequent faults (as fully included in update to Chapter 16.5 of the PCSR)	21
GI-UKEPR-CI-06.A9	Sensor Diversity	PELA-F DC 3 Rev C	Diversity implementation plan for sensors and conditioning	33
GI-UKEPR-CI-06.A9	Sensor Diversity	PEPS-F DC 90 Rev C	Safety principles applied to UK EPR™ I&C Architecture in terms of the requirements for diversity and independence	34
GI-UKEPR-CI-06.A9	Sensor Diversity	PEPS-F DC 148 Rev A	Allocation of sensors and conditioning when three lines of defence are involved	35
GI-UKEPR-CI-06.A9	Sensor Diversity	PELL-F DC 82 Rev C	Diversity criteria for sensors and conditioning	36
GI-UKEPR-CI-06.A9	Sensor Diversity	PEPR-F DC 83 Rev C	Functional Analysis for sensors common cause failure	37

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Topic	Document Ref.	Title	Ref.
GI-UKEPR-CI-06.A9	Sensor Diversity	ECEF091489 Rev E	Classification of I&C safety features	38
GI-UKEPR-CI-06.A9	Sensor Diversity	CMF-64	C&I diversity on sensors and sensor conditioning	8
GI-UKEPR-CI-06.A9	Sensor Diversity	CMF-67	Addition of secondary side pressure measurements	8
GI-UKEPR-CI-06.A9	Sensor Diversity	PEPRF.12.0855	Answer to TQ-EPR-1578 (sensor diversity)	39
GI-UKEPR-CI-06.A9	Actuator Diversity	ECESN120472 Rev A	Diversity implementation plan for PACS Modules	41
GI-UKEPR-CI-06.A9	Actuator Diversity	CMF-65	C&I diversity on PACS modules	8
GI-UKEPR-CI-01.A1	NCSS functional specification	NEPR-F DC 551 Rev C	Function requirements on Non Computerised safety I&C functions	42
GI-UKEPR-CI-01.A1	NCSS functional specification	PEPR-F DC 105 Issue A	Functional justification of the Non Computerised Safety System design (Response to TQ-EPR-1567)	43
GI-UKEPR-CI-01.A1	NCSS functional specification	PEPRF12.0966	Spurious opening of a Pressuriser Safety Valve in case of loss of computerised I&C (Response to TQ-EPR-1567)	44
GI-UKEPR-CI-01.A1	NCSS functional specification	PEPRF12.1062	Comparison of the NCSS functions and SAS diversified functions (Response to TQ-EPR-1567)	45
GI-UKEPR-CI-01.A1	NCSS functional specification	CMF-14	NCSS design	8

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – EDF and AREVA Deliverables

GDA Issue Action	Fault Studies Topic	Document Ref.	Title	Ref.
GI-UKEPR-CI-01.A1	NCSS functional specification	CMF-68	Non computerised Safety System Design Improvements	8
GI-UKEPR-CC-01.A1	Classification of CVCS	NEPS-F DC 557 Rev D	Methodology for Classification of Structures, Systems, Safety Features and Component	47
GI-UKEPR-CC-01.A1	Classification of CVCS	CMF-24	Implementation of NEPS-F DC 557	8
GI-UKEPR-CC-01.A1	Classification of CVCS	Letter EPR01157R	Classification of CVCS	48
GI-UKEPR-CC-01.A1	Classification of CVCS	Letter EPR01403N	Supplemental Response to TQ-EPR-1630	49
GI-UKEPR-CC-01.A1	Classification of CVCS	CMF-33	Implementation of an automatic Class 1 signal “isolation of CVCS letdown line in case of high activity in the primary coolant”	8
GI-UKEPR-CC-01.A5	Diverse Lines of Protection	CMF-36	Diverse lines of protection	8
GI-UKEPR-CC-01.A5	Classification of SBO diesels	CMF-37	Upgrade of Ultimate Diesel Generators	8

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1539	GI-UKEPR-FS-02.A6	PEPR-F 11.0956	Comments on loss of CVCS faults
TQ-EPR-1555	GI-UKEPR-CI-06.A9	PELA-F DC 3 Rev A PEPR-F DC 83 Rev A	Diversity Implementation Plan
TQ-EPR-1567	GI-UKEPR-CI-01.A1	NEPR-F DC 551 Rev B	Comments on NCSS Functional Requirements
TQ-EPR-1578	GI-UKEPR-CI-06.A9	PELA-F DC 3 Rev A PELL-F DC 82 Rev B PEPR-F DC 83 Rev A	Comments on Sensor Diversity
TQ-EPR-1569	GI-UKEPR-CC-01.A6	TQ-EPR-1515	Response to TQ-EPR-1515
TQ-EPR-1579	GI-UKEPR-FS-02.A9	NEPR-F DC 580 Rev B	Comments on Diversity to Safe Shutdown State
TQ-EPR-1581	GI-UKEPR-FS-02.A5	PEPCF.11.1467 Rev A	Comments on Rod Misplacement Faults
TQ-EPR-1593	GI-UKEPR-FS-02.A2	PEPR-F DC 84 Rev A	Comments on Excessive Increase in Steam Flow
TQ-EPR-1595	GI-UKEPR-FS-02.A9	PEPRF.11.1349	Definition of Non Hazardous Stable State
TQ-EPR-1615	GI-UKEPR-CC-01.A1	Letter EPR01157R	Classification of the CVCS

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-FS-02 Revision 0 – Diversity for Frequent Faults – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1621	GI-UKEPR-FS-02.A8	ECESN120355 Rev A PEPR-F DC 103 Rev A	Loss of support systems
TQ-EPR-1630	GI-UKEPR-CC-01.A1	TQ-EPR-1615	Safety Injection Diversity and Classification of the CVCS

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-41	The future licensee shall demonstrate that the ex-core neutron flux detectors are functionally capable of providing diverse protection against excessive increase in secondary steam flow faults including spurious lifting of the Main Steam Relief Train (MSRT) valves so as to avoid Departure from Nucleate Boiling (DNB).	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-42	The future licensee shall demonstrate that the in-core Self-Powered Neutron Detectors (SPND) are functionally capable of protecting against Rod Cluster Control Assembly (RCCA) misalignment faults including one or more dropped RCCAs and against uncontrolled single RCCA withdrawal faults assuming the loss of the most onerous SPND finger due to a single failure such that DNB is avoided using conservative PCC analysis rules and conservative methods and assumptions.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-43	The future licensee shall explore the feasibility of using the axial offset signal on the ex-core detectors as a diverse means of ensuring the reactor is sufficiently well trimmed so as to avoid entering DNB following RCCA misplacement faults including the dropping of more than one RCCA together with common mode failure of the SPNDs.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-44	The future licensee shall determine which of the options identified within Change Management Form (CMF) #59 is to be developed into fully worked up proposal to provide diverse protection against homogeneous boron dilution faults occurring during shutdown conditions.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-45	The future licensee shall perform a functional diversity analysis for all frequent faults considering the common mode failure of each of the essential support systems to demonstrate that adequate functional diversity is provided.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-46	The future licenses shall provide a fully integrated safety case for the station blackout sequence.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-47	The future licensee shall review the definition of the controlled state against the definition of the non-hazardous stable state to ensure that the categorisation of reactivity control function (and classification of associated systems responsible for RCS boration) is appropriate.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-48	The future licensee shall perform an ALARP assessment on the feasibility of providing a diverse means of isolating one pair of steam lines from the other pair following a break on the secondary side.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-49	The future licensee shall demonstrate diverse protection for frequent cold overpressure faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-50	The future licensee shall review the demonstration of functional diversity for frequent faults to ensure it is applicable for plant states.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-51	The future licensee shall perform an ALARP assessment on the feasibility of tripping the main feedwater pumps as a diverse means of ensuring feedwater isolation.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-52	The future licensee shall review the implications of assuming plant maintenance states on the demonstration of functional diversity for frequent initiating events unless it can be shown that the sequence frequency is below 10^{-7} per year.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-53	The future licensee shall update the PCSR to reflect the definition of controlled state for fuel pool faults, the functioning of the RCSL anti-dilution safety function, the change in protection claimed for excessive increase in secondary steam flow faults with failure of PS and the inclusion of support system functions in the fault and protection schedule.	Fuel on Site
AF-UKEPR-FS-54	The future licensee shall complete the work on demonstration of functional diversity for sensors and conditioning modules by including consideration of support system faults, spent fuel pool faults, frequent internal and external hazards, boron dilution faults and the revised safety case for excessive increase in secondary steam flow faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-55	The future licensee shall consider the feasibility of providing a diverse reactor trip and safety injection signal on the SAS based upon a high containment pressure signal.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-56	The future licensee shall consider the feasibility of providing a diverse reactor trip and safety injection signal on the SAS based upon detection of the existing low cold leg temperature signal.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-57	The future licensee shall provide justification for not providing a diverse reactor trip signal on the SAS based upon detection of turbine trip signal.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-58	The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of low RCP current.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-59	The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of low RCP voltage.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-60	The future licensee shall consider the feasibility of providing a diverse reactor trip signal on the SAS based upon detection of the existing low SG pressure signal.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-61	The future licensee shall develop a PSA model of the UK EPR™ C&I systems to adequately assess the impact on risk of the allocation of sensors, conditioning modules and PACS modules, especially in terms of dependency.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-62	The future licensee shall provide justification for those functions on the SAS and NCSS for which reliance will be placed upon manual actuations.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-63	The future licensee shall provide transient analysis studies to demonstrate that there is adequate diverse protection against the loss of one RCP.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-64	The future licensee shall provide transient analysis studies to demonstrate that there is adequate diverse protection against the uncontrolled single RCCA withdrawal fault.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-65	The future licensee shall review the allocation of conditioning modules for the in-core and ex-core detectors to reduce the risk to ALARP of both systems being unavailable following common failure of a single design of conditioning module.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-66	The future licensee shall perform a review of the allocation of conditioning modules using the PSA model developed under **AF-UKEPR-FS-61** taking into account plant maintenance states and provide a technical justification for excluding consideration of the most onerous plant maintenance state within the safety principles applied to the UK EPR™ C&I architecture.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-67	The future licensee shall review and update the C&I safety features classification document to ensure diverse C&I systems are appropriately classified.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-68	The future licensee shall perform a review of the allocation of PACS modules using the PSA model developed under **AF-UKEPR-FS-61** taking into account plant maintenance states.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-69	The future licensee shall review all valve and motor actuations to ensure that the design logic is such that common mode failure of a PACS module cannot result in the failure of two diverse systems both contributing to the same safety function. Consideration also needs to be given to common mode failure of the PS resulting in a spurious signal that overrides a correct signal from the SAS/NCSS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-70	The future licensee shall complete the analysis work required to fully define the functional specification of the Non-Computer based Safety System (NCSS). This includes verification of effectiveness of the claimed reactor trip signals, design of automatic thresholds, definition of response time together with required accuracy, remaining faults including SGTR, support systems, and fuel pool faults, design of support system actuators, analyses of severe accident mitigation, and information needs in MCR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-71	The future licensee shall consider the feasibility of providing a manual actuation function on the NCSS of the Extra Boration System (EBS).	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-72	The future licensee shall clarify whether reference to the Emergency Diesel Generators (EDG) made in the justification of the functional specification for the NCSS for the case of loss of off-site power is correct or provide an alternate justification for this fault sequence.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 2

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-02 Rev 0

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-73	The future licensee shall consider the feasibility for providing the capability for manually actuating the stand-still seal system on the NCSS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-74	The future licensee shall confirm that the high hot leg pressure signal on the NCSS is functionally capable of providing protection against the spurious closure of all four MSIVs with failure of the computer based C&I systems.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-75	The future licensee shall demonstrate that hot leg injection provides an adequate diverse means of safety injection for frequent SBLOCA faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UKEPR-FS-76	The future licensee shall present its proposed maintenance arrangements for Class 3 duty systems such as the CVCS.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

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

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

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A1**
GDA Issue	Demonstration of functional diversity for frequent faults		
GDA Issue Action	Implement the proposed modification to provide a diverse high hot leg pressure trip signal on an appropriately diverse protection system for a loss of normal feedwater fault with failure of the reactor protection system to trip. EDF and AREVA have identified that a modification is required to provide a reactor trip signal on high hot leg pressure on a non-TXS based protection system. This is to protect against a loss of normal feedwater fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A2**
GDA Issue Action	Provide improved protection for the excessive increase in secondary steam flow fault with failure of the reactor to trip due to either mechanical failure of the RCCAs to insert or failure of the reactor protection system. In NEPR-F DC 592, analysis is presented for the case of excessive increase in secondary steam flow with failure of the reactor to trip. The analysis demonstrates that for such transients, the fault continues for a considerable period and that the variation in DNB is significant. This is true for both the mechanical failure of the RCCAs to insert and the failure of the TXS-based reactor protection system: • In the case of the mechanical failure to insert, the position has been made worst by the recent design change to increase the partial cooldown rate for SBLOCA faults which has resulted in a relaxation of the SG pressure drop trip set point which now means that low SG level is the most effective trip parameter for these faults. • In the case of mechanical failure of the RCCAs to insert, EDF and AREVA will justify why it is not ALARP to provide an additional trip signal or tighten the protection set points for this fault. • In the case of TXS failure, EDF and AREVA will perform an ALARP study to explore the feasibility of providing an extra trip parameter on a non-TXS based diverse protection system. Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A3**
GDA Issue Action	Implement the proposed modification to provide a diverse low RCP speed trip signal on an appropriately diverse protection system for a reduction in flow fault with failure of the reactor protection system to trip. EDF and AREVA have identified that a modification is required to provide a reactor trip signal on low RCP speed on a non-TXS based protection system. This is to protect against a flow reduction fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area	**FAULT STUDIES**		
Related Technical Areas	Probabilistic Safety Assessment Control and Instrumentation Human Factors		
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A4**
GDA Issue Action	Implement the proposed modification to provide diverse high axial offset and high neutron flux trips on an appropriately diverse protection system for a RCCA bank withdrawal fault with failure of the reactor protection system to trip. EDF and AREVA have identified that two extra reactor trip signals need to be added to a non-TXS based protection system. The extra trip signals are a high axial offset trip and a high neutron flux trip. These changes are to protect against a RCCA bank withdrawal fault with failure of the TXS based reactor protection system to trip the reactor. The design for the proposed modification will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A5**
GDA Issue Action	Demonstrate the provision of diverse protection against RCCA misplacement faults including one or more dropped RCCAs. No analysis of these faults is presented within NEPR-F DC 592 and yet these faults will be very difficult to detect should there be a failure of the TXS-based reactor protection system. For this reason, EDF and AREVA are to provide explicit transient analysis using design basis analysis techniques for these faults to demonstrate that the diverse protection systems are functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a negative-rate flux trip signal on a non TXS-based protection system is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A6**
GDA Issue Action	Demonstrate the provision of diverse protection against loss of CVCS following a normal reactor trip and xenon decay including demonstration of diversity to operator action. After every reactor trip from full power there is an eventual decay in the level of xenon poisoning within the reactor core. The resultant swing in reactivity needs to be compensated for through increasing the boron concentration in the reactor to ensure an adequate shutdown margin. While the emergency boration system (EBS) and the in-containment refuelling water storage tank (IRWST) provide two diverse sources of borated water, should the operator fail to ensure adequate shutdown margin using the Chemical and Volume Control System (CVCS), both these systems are also dependent upon operator action for actuation. Although timescales are long (many hours), this implies a combined human reliability of 1×10^{-7} per demand to meet the design basis target. For this reason, EDF and AREVA are to provide an ALARP study into the feasibility of automatically actuating the CVCS system to inject borated water after every reactor trip and for the EBS to be automatically actuated following failure of the CVCS. Alternatively, EDF and AREVA may wish to provide a consequence analysis of what would happen should the operator fail to ensure adequate shutdown margin. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A7**
GDA Issue Action	Demonstrate the provision of diverse protection against a homogenous boron dilution fault occurring in shutdown conditions with failure of the reactor protection system. No analysis of this fault is presented within NEPR-F DC 592 and yet such a fault would be very difficult to detect should there be a failure of the TXS-based reactor protection system. For this reason, EDF and AREVA are to provide explicit transient analysis using design basis analysis techniques for this fault to demonstrate that the diverse protection systems are functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a boron dilution block signal and an EBS actuation signal on a non TXS-based protection system (actuated by low doubling time and/or high source-range flux level) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A8**
GDA Issue Action	Demonstrate the provision of diverse protection for the frequent faults involving the loss of essential support systems (e.g. loss of cooling chain, electrical, HVAC). EDF and AREVA are to provide a demonstration of diversity for frequent faults involving loss of essential support systems including loss of cooling chain, electrical and HVAC systems. EDF and AREVA are to demonstrate that any diverse systems claimed are appropriately categorised. In the case of loss of grid with failure of the TXS-based protection system, the feasibility of automatically actuating the station-blackout diesel generators (SBO DGs) on a non-TXS based protection system will need to be considered as a possible ALARP measure. Any design changes identified from the review will need to complete the six-stage modification process for inclusion within the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-FS-02 Revision 0 – Fault Studies – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY FOR FREQUENT FAULTS

GI-UKEPR-FS-02 REVISION 0

Technical Area		**FAULT STUDIES**	
Related Technical Areas		Probabilistic Safety Assessment Control and Instrumentation Human Factors	
GDA Issue Reference	**GI-UKEPR-FS-02**	**GDA Issue Action Reference**	**GI-UKEPR-FS-02.A9**
GDA Issue Action	Demonstrate that there exists a diverse means of achieving the safe shutdown state from the controlled state for frequent faults. EDF and AREVA are to demonstrate that diverse means of achieving a safe shutdown state from the controlled state exist for all frequent faults and that all structures, systems and components are appropriately categorised. Any design changes required because of any reclassifications will need to complete the six-stage modification process for inclusion in the consolidated PCSR. With agreement from the Regulator this action may be completed by alternative means.		