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-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims

Assessment Report: ONR-GDA-AR-12-009
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 Human Factors (HF). This report specifically addresses the GDA Issue (**GI-UKEPR-HF-01**) and associated GDA Issue Actions generated as a result of the GDA Step 4 HF Assessment of the UK EPR™. It only presents the assessment undertaken as part of the resolution of the GDA Issue and it is recommended that it be read in conjunction with the reports of previous Steps of the GDA process relating to HF of the EDF and AREVA UK EPR™ in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process.

The Step 4 HF GDA Issue related to inadequate substantiation of Human Based Safety Claims (HBSCs) and omission of a consolidated HF safety case for the UK EPR. It required EDF and AREVA to:

- Complete the identification and substantiation of pre-fault and post-fault human failure events.
- Provide holistic arguments for key elements of the UK EPR™ operation.
- Provide evidence on how the design of the UK EPR™ prevents and mitigates the potential for violations.
- Provide a consolidated HF safety case in a revision of the Pre-Construction Safety Report (PCSR).

EDF and AREVA have undertaken considerable work to complete identification and substantiation of risk significant pre-fault (Type A and B) and post-fault (Type C) Human Failure Events (HFEs). It has provided additional qualitative arguments to support its case on the identified key topics supported by evidence stemming from the analyses undertaken. It has provided a consolidated HF safety case in a significant revision of the PCSR, notably a revised Chapter 18 that presents the main HF safety case.

I consider that the identification and substantiation of risk significant Type A and B pre-fault HFEs has been completed as far as is reasonably practicable at this point although further work will be required by a future licensee as the detailed design progresses. I judge that the substantiations provided are based on reasonable assumptions about the detailed design, maintenance and operations, including the supporting procedures.

I consider that substantiation of all risk significant (i.e. the high and medium risk) Type C post-fault HFEs has been provided. However I consider that only a few of the Type C HFEs have been fully substantiated; the majority of these HFEs have only been partially substantiated. In these cases I judge that an acceptable position for these HFEs should be straightforward to achieve during the site specific phase. EDF and AREVA have identified and recorded the issues and assumptions requiring further consideration or implementation by a future licensee.

I consider that EDF and AREVA have provided satisfactory holistic arguments and evidence consistent with the generic design phase on:

- The prevention of misdiagnosis and design related violations; and
- The failure of Process Information and Control System (PICS), including the Automatic Diagnosis feature and the transfer to Safety Information and Control System (SICS) or Non Computerised Safety System (NCSS) operation.

A number of detailed HF issues and key underpinning assumptions need to be considered further or implemented by a future licensee. Most of these have been identified by EDF and AREVA and are in their HF Issues and Assumptions registers. I have encompassed all these within a small

number of Assessment Findings (AF) that, in conjunction with the AFs identified at GDA Step 4, will need to be addressed by a future licensee.

I consider that the submissions provided along with the material presented for GDA Step 4 now comprise a satisfactory HF safety case for the UK. This has been summarised and presented in a significant revision of the PCSR, primarily in a revised Chapter 18, which provides a clear presentation of all the significant claims, arguments and supporting evidence.

I conclude that EDF and AREVA have:

- Adequately addressed each specific part of the GDA Issue **GI-UKEPR-HF-01**.
- Developed a satisfactory HF safety case that matches UK expectations.
- Provided a revised Chapter 18 of the UK EPR™ PCSR which now provides an acceptable summary of this overall HF safety case.

I am satisfied that the GDA Issue generated as a result of the GDA Step 4 HF Assessment can be closed and that there are no areas for resolution that prevent construction of the UK EPR™ within the UK.

LIST OF ABBREVIATIONS

AD	Automatic Diagnosis
AF	Assessment Finding
ALARP	As Low As Reasonably Practicable
BF	Bounding Fault
CAD	Computer Aided Design
CCWS	Component Cooling Water System
CHRS	Containment Heat Removal System
CMF	Change Management Form
CoT	Core outlet Temperature
CSF	Critical Safety Function
CVCS	Chemical and Volume Control System
C&I	Control and Instrumentation
DG	Diesel Generator
ED	Emergency Director
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System
EPRI	Electric Power Research Institute
ESWS	Essential Service Water System
FA	Fuel Assembly
FA3	Flamanville 3
FO	Field Operator
FSCD	Fast Secondary Cooldown
FV	Fussel-Vesely
GDA	Generic Design Assessment
HAZOP	Hazard and Operability study
HBD	Heterogeneous Boron Dilution
HBSC	Human Based Safety Claim
HD	Diesel Building
HEP	Human Error Probability
HF	Human Factors
HFAR	Human Factors Assumptions Register
HFE	Human Failure Event

LIST OF ABBREVIATIONS

HFIR	Human Factors Issues Register
HK	Fuel Building
HL	Safeguards Building
HMI	Human Machine Interface
HR	Reactor Building
HRA	Human Reliability Analysis
HSE	Health and Safety Executive
IE	Initiating Event
INPO	Institute of Nuclear Power Operations
IRWST	In-Containment Refuelling Water Storage Tank
JPI	Nuclear Island Fire Fighting Water Distribution System
JPV	Diesel Building Fire Fighting Water Distribution System
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accident
LOOP	Loss of Offsite Power
LTP	Local to Plant
LUHS	Loss of Ultimate Heat Sink
MCR	Main Control Room
MFWS	Main Feedwater System
MOP	Manual Operating Procedure
MSRT	Main Steam Relief Train
NAB	Nuclear Auxiliary Building
NCSS	Non Computerised Safety System
NPP	Nuclear Power Plant
OA	Operator Action
ONR	Office for Nuclear Regulation (an agency of HSE)
OpEx	Operational Experience
OS	Operator Strategy
OSSA	Operating Strategy for Severe Accidents
PC	Primary Circuit
PCSR	Pre-Construction Safety Report
PDS	Primary Depressurisation System
PICS	Process Information and Control System
PM	Preventative Maintenance

LIST OF ABBREVIATIONS

POP	Plant Overview Panel
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSIS	Inter Panel Signalisation Panel
PTR	Fuel Pool Cooling System
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RIF	Risk Increase Factor
RM	Refuelling Machine
RPV	Reactor Pressure Vessel
RT	Reactor Trip
SAB	Safeguard Building
SAP	Safety Assessment Principle(s) (HSE)
SBO	Station Blackout
SE	Safety Engineer
SEC	Essential Service Water System
SED	pH7 Demineralised Water Distribution System
SEP	Drinking Water Distribution System
SFP	Spent Fuel Pond
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SICS	Safety Information and Control System
SME	Subject Matter Expert
SOA	State Orientated Approach
SS	Shift Supervisor
SSS	Start-up and Shutdown System
SSSS	Stand Still Seal System
TA	Task Analysis
TTA	Tabular Task Analysis
TAG	Technical Assessment Guide(s) (ONR)
TSC	Technical Support Contractors
TQ	Technical Query
TXS	Teleperm XS

LIST OF ABBREVIATIONS

UK	United Kingdom
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 Background

1 This report presents the Close-out of the Office for Nuclear Regulation (ONR), an agency of the Health and Safety Executive (HSE), Generic Design Assessment (GDA) within the area of Human Factors. The report specifically addresses the GDA Issue **GI-UKEPR-HF-01 Revision 0** and associated GDA Issue Actions (see Annex 3 that reproduces (Ref. 6) generated as a result of the GDA Step 4 HF Assessment of the EPR™ (Ref. 7)). My assessment has focussed on the deliverables identified within the EDF and AREVA Resolution Plan (Ref. 8) published in response to the GDA Issue.

2 GDA followed a step-wise-approach in a claims-argument-evidence hierarchy. GDA Step 1 was a preparatory stage with no actual assessment undertaken. In GDA Step 2 the claims made by EDF and AREVA were examined and in GDA Step 3 the arguments that underpin those claims were examined. GDA Step 4 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. In the technical area of HF, no assessment was undertaken in GDA Step 2, and the GDA Step 3 Assessment Report was more aligned to a GDA Step 2 Assessment Report; focusing on consideration of EDF and AREVA's claims, with very limited consideration of the available arguments. As a result the assessment was back-loaded to GDA Step 4, during which the arguments and supporting evidence for the Human Based Safety Claims (HBSC) were examined in detail.

3 The GDA Step 4 HF Assessment identified one GDA Issue and a number of Assessment Findings (AF). GDA Issues are unresolved issues considered by regulators to be significant, but resolvable, and which require resolution before nuclear island safety related construction of such a reactor could be considered. AFs are findings that are identified during the regulators' GDA assessment that are important to safety, but not considered critical to the decision to start nuclear island safety related construction of such a reactor.

4 The overall GDA Step 4 Assessment concluded that the UK EPR™ reactor was suitable for construction in the UK subject to resolution of 31 GDA Issues. The purpose of this report is to provide the assessment which underpins the judgement made in closing GDA Issue **GI-UKEPR-HF-01**.

1.2 Scope

5 This report presents only the assessment undertaken as part of the resolution of the GDA Issue **GI-UKEPR-HF-01** and it is recommended that this report be read in conjunction with my GDA Step 4 HF Assessment of the EDF and AREVA UK EPR™ (Ref. 7) in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process.

6 The overall judgement of my GDA Step 4 HF Assessment (Ref. 7) was that an adequate safety case for HF had not been made for the EDF and AREVA UK EPR™; and the position had not moved on significantly from the end of GDA Step 3.

7 Much of the material that was available for assessment during GDA Step 4 was extracted from documentation related to the Flamanville 3 (FA3) design and was therefore not directly pertinent to the UK EPR™. No consolidated HF safety case aligned with UK regulatory expectations was provided. Four UK EPR™ specific qualitative analyses were provided to substantiate Human Based Safety Claims (HBSC) during GDA Step 4.

However, these amounted to only a very small part of the required substantiation for the entirety of HBSCs for the UK EPR™.

8 This was inadequate for a Pre-Construction Safety Report (PCSR) and represented a substantial gap in the safety submission for GDA remaining at the end of GDA Step 4. As a result I raised the GDA Issue **GI-UKEPR-HF-01** to require EDF and AREVA to substantiate the HBSCs and to provide a consolidated HF safety case for the UK EPR. The Issue only required qualitative aspects of the HBSCs to be considered; consequently associated numerical HRA and PSA issues have not been re-visited as part of the Close-out work. AFs I raised at Step 4 on the HRA will ensure that these aspects are considered post-GDA.

9 This 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 the GDA Issue highlight shortfalls not previously identified during GDA Step 4, these will be addressed as part of the Close-out phase or be identified as AFs to be taken forward to the site specific phase. Additionally design changes arising from response to close-out other GDA Issues have been considered if they have impacted aspects of the HF safety case assessed at Step 4.

10 Where aspects of the assessment are judged to require further detailed evidence when the information becomes available at a later stage new AFs have been raised. These are added to those previously identified at GDA Step 4 to be addressed by a future licensee seeking to construct a UK EPR™.

1.3 Methodology

11 The methodology applied to this assessment continues the approach taken during GDA Step 4 which followed the ONR document HOW2 PI/FWD – Issue 3 (Ref. 1), in relation to mechanics of assessment within the Office for Nuclear Regulation (ONR).

12 This assessment has been focussed primarily on the submissions relating to resolution of the GDA Issue **GI-UKEPR-HF-01** as well as any further requests for information or justification derived from assessment of those submissions.

13 Analysis work to resolve GDA Issue **GI-UKEPR-HF-01** has included HF studies that support the safety cases for closure of other GDA Issues. These have been in the Fault Studies and Internal Hazards disciplines; specifically **GI-UKEPR-FS-01** on Heterogeneous Boron Dilution faults, **GI-UKEPR-FS-02** on Diversity for Frequent Faults, **GI-UKEPR-FS-04** Steam Generator Tube Rupture Safety Case, **GI-UKEPR-IH-01** Dropped Loads and Impact; and **GI-UKEPR-IH-03** Internal Flooding and Operator Actions. Consideration of the HF aspects of these GDA Issues is presented within their individual GDA Issue Close-out reports. The detailed assessment of the HF studies is considered within this report.

14 The aim of this assessment is to provide a comprehensive assessment of the submissions provided in response to the GDA Issue to enable ONR to gain confidence that the concerns raised have been resolved so that they can be closed. Where requirements for more detailed evidence have been identified that are appropriate to be provided at the design, construction or commissioning phases of a site specific project these can be carried forward as AFs.

1.4 Report Structure

15 The structure of this report is as follows:

- Section 1 (this section) – provides the background to the GDA process, the origination of the GDA Issue **GI-UKEPR-HF-01**, defines the scope of the GDA Close-out assessment and outlines the assessment method.
- Section 2 – defines my Assessment Strategy for the GDA Close-out, identifies the standards and guidance materials that have been used and notes what aspects have been considered to be out of scope.
- Section 3 – outlines the submissions provided by EDF and AREVA in response to GDA Issue **GI-UKEPR-HF-01** against the specific GDA Issue Actions (a complete list of submissions along with details of regulatory communication via Technical Query (TQ) and letters is provided at Annex 1).
- Section 4 – presents my assessment of EDF and AREVA's submissions in response to **GI-UKEPR-HF-01** as well as that relating to the HF contribution to the closure of GDA issues from other technical disciplines. AFs arising from this assessment are presented within this section alongside the relevant assessment text and are collated in Annex 2. Further detailed assessment information on the substantiation of particular Type C (post fault) HBSCs is presented in Annex 4.
- Section 5 – summarises my review of the updated UK EPR™ PCSR. As action A2 of **GI-UKEPR-HF-01** required the development of a new consolidated HF safety case I have considered this throughout my assessment (as recorded in Section 4). Section 5 therefore provides a summary of this assessment.
- Section 6 – collates the AFs from my assessment and also records those previously identified during GDA Step 4 that have been impacted by the work to Close-out **GI-UKEPR-HF-01**.
- Section 7 – provides the overall conclusions resulting from my assessment and includes my final judgement regarding closure of GDA Issue **GI-UKEPR-HF-01**.
- Annex 1 provides details of the EDF and AREVA submissions in response to the GDA Issue; along with TQs and key correspondence.
- Annex 2 lists the AFs arising from this Close-out assessment.
- Annex 3 presents the GDA Issue **GI-UKEPR-HF-01**.
- Annex 4 gives a summary of my assessments of the main Type A, B and C Human Failure event (HFE) submissions.
- Annex 5 gives a summary of my assessment of the HF assessments for Dropped Loads and Internal Flooding.

2 ONR'S ASSESSMENT STRATEGY FOR HUMAN FACTORS

16 My assessment strategy for GDA Close-out for the HF topic area has continued the approach taken for the GDA Step 4 assessment, including use of the relevant standards and criteria. This effectively continues and completes the assessment envisaged for Step 4 that had to be curtailed due to the lack of submissions.

17 The HF assessment approach at GDA Step 4 focused on five key work streams that addressed the breadth of HF within a PCSR. The work streams were:

- Work stream 1: Substantiation of human based safety actions.
- Work stream 2: Generic Human Reliability Assessment.
- Work stream 3: Engineering systems.
- Work stream 4: HF Integration.
- Work stream 5: Plant wide generic HF assessment.

18 At the end of GDA Step 4 four of these work streams were judged to be acceptable. The key work stream giving rise to the GDA Issue was work stream 1 on assessing the identification and substantiation of HBSCs. The HF assessment for the Close-out of **GI-UKEPR-HF-01** therefore focuses primarily on this work stream. However, where elements of other work streams are relevant to a claim (e.g. the use of novel Human Machine Interfaces (HMI)) the resultant assessment has considered criteria relating to the other work stream accordingly.

19 The overall bases for the assessment of the GDA Issue are the HF elements of:

- Submissions made to ONR in accordance with the resolution plan for **GI-UKEPR-HF-01**; this includes HF submissions supporting Close-out of other GDA Issues.
- Responses to TQs that were raised during the GDA Close-out assessment process.
- Updates to the Submissions / PCSR / Supporting Documentation.

2.1 The Approach to Assessment for GDA Close-out

20 The overall approach to the closure of GDA Issue **GI-UKEPR-HF-01** for the UK EPR™ project involved:

- Assessment of initial submissions made by EDF and AREVA in response to the GDA Issue. These submissions are detailed within the EDF and AREVA Resolution Plan for **GI-UK-EPR-HF-01**.
- Providing regulatory comment on initial submissions so that EDF and AREVA were able to update the submission such that it better met regulatory expectations.
- Generation of TQs in the event of requiring further supporting evidence for the assessment or to raise a particular concern.

21 My assessment was selected, targeted and proportionate to the relative importance of the claims and / or contribution to the overall HF safety case. The programme of work and timing of submissions that I agreed with EDF and AREVA was devised to provide me with assurance that the GDA Issue would be fully addressed. Early submissions related to analytical methodologies and approaches so that I could be assured that these were appropriate. Additionally EDF and AREVA provided early examples of the implementation of these methodologies for the substantiation of Type A & B errors, and for Type C actions.

22 I also adopted this approach for the assessment of the revised PCSR HF safety case as required by Action A2 of **GI-UKEPR-HF-01**. A significant revision of the previous PCSR Chapter 18 was needed to present the final consolidated safety case. The agreed programme allowed early sight of EDF and AREVA's proposed PCSR chapter revision through the provision of early interim submissions.

23 Annex 1 contains detailed tables of documents assessed, letters providing regulatory comment and TQs raised as a result of the HF assessment.

2.2 Standards and Criteria

24 The relevant standards and criteria adopted within this Assessment mirror those used at GDA Step 4; primarily those for work streams 1 and 5. These are principally the Safety Assessment Principles (SAP), internal ONR Technical Assessment Guides (TAG), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant TAGs are shown in Table 1 below. National and international standards and guidance have been referenced where appropriate within this report. Other relevant good practice, where applicable, has also been cited within the body of this report.

2.2.1 Safety Assessment Principles and Technical Assessment Guides

25 The SAPs and TAGs applied within the assessment to Close-out GDA Issue **GI-UKEPR-HF-01** are included within Table 1. This includes SAPs and TAGs that focus explicitly on HF, and others that include some aspect relevant to HF.

Table 1: Safety Assessment Principles and Technical Assessment Guides used as an Assessment Basis for GDA Close-out of **GI-UKEPR-HF-01** Revision 0

Work Stream	Relevant HF SAP applied	Relevant non-HF SAP applied	Relevant TAG applied
Work Stream 1 – Substantiation of human based safety actions	EHF.2 EHF.3 EHF.4 EHF.5 EHF.6 EHF.10	SC.4 SC.6 EKP.1 EKP.2 EKP.3 EKP.4 EKP.5 ESS.9 FA.7 NT.2	T/AST/005 – ND Guidance on the demonstration of ALARP (Ref. 3). T/AST/010 – Early initiation of safety systems (Ref. 3) T/AST/051 – Guidance on the purpose, scope and content of Nuclear Safety Cases (Ref. 3). T/AST/063 – Human Reliability Analysis (Ref. 3).
Work Stream 2 – Generic Human Reliability Assessment	EHF.5 EHF.7 EHF.10	SC.5 ERL.1 FA.13	T/AST/063 – Human Reliability Analysis (Ref. 3).
Work Stream 3 – Engineering systems	EHF.1 EHF.2 EHF.3 EHF.6 EHF.7 EHF.10	ECS.3 ECS.5 ERL.2 EMT.1 EMT.4 EMT.6 ELO.1 EMC.8 ESS.15 ESS.26	T/AST/009 – Maintenance, inspection and testing of safety systems, safety-related structures and components (Ref. 3). T/AST/058 – Human Factors Integration (Ref. 3). T/AST/059 – Human Machine Interface (Ref. 3).

Table 1: Safety Assessment Principles and Technical Assessment Guides used as an Assessment Basis for GDA Close-out of **GI-UKEPR-HF-01** Revision 0

Work Stream	Relevant HF SAP applied	Relevant non-HF SAP applied	Relevant TAG applied
Work Stream 4 – Human Factors Integration	EHF.1 EHF.2 EHF.3 EHF.4 EHF.5 EHF.6 EHF.7 EHF.8 EHF.9 EHF.10	MS.4 SC.4 SC.7	T/AST/005 – ND Guidance on the demonstration of ALARP (Ref. 3). T/AST/058 – Human Factors Integration (Ref. 3).
Work Stream 5 – Plant-wide generic Human Factors assessment	EHF.1 EHF.2 EHF.3 EHF.4 EHF.5 EHF.6 EHF.7 EHF.8 EHF.9 EHF.10	SC.4 EKP.1 EKP.4 ELO.1 ESS.3 ESS.13 ESS.14 ESS.15 ESR.1	T/AST/059 – Human Machine Interface (Ref. 3).

2.3 Use of Technical Support Contractors

26 Technical Support Contractors (TSC) were not used for the HF assessments during the GDA Close-out of **GI-UKEPR-HF-01**.

2.4 Out-of-scope Items

27 The following items have been agreed with EDF and AREVA as being outside the scope of GDA for HF:

- team organisation;
- staffing;
- operating and maintenance procedures;
- use of State Orientated Approach (SOA);
- display breakdown; and
- training.

28 EDF and AREVA have made key assumptions about some of the above out of scope items in their GDA submissions in order to substantiate claimed HBSCs. These assumptions effectively form a set of requirements or expectations that need to be fulfilled by a future licensee or it will need to provide a justification for any alternative position. Several notable elements have been embedded within the substantiation of HBSCs for GDA; hence any future licensee wishing to adopt alternative approaches would be required to justify the changes. These elements are:

- The application of the SOA, and procedures for abnormal operations.

- The Main Control Room (MCR) staffing philosophy comprising a Strategy Operator (OS), Action Operator (OA), Supervisor (SS) and Safety Engineer (SE).

3 EDF AND AREVA DELIVERABLES IN RESPONSE TO GI-UKEPR-HF-01

3.1 Introduction

29 In response to **GI-UKEPR-HF-01** EDF and AREVA provided a Resolution Plan (Ref. 8), that provides specific deliverables to address each discrete element of the two main GDA Issue Actions. Action **GI-UKEPR-HF-01.A1** relates to substantiation of UK EPR™ HBSCs; Action **GI-UKEPR-HF-01.A2** requires provision of a consolidated HF safety case and update for the UK EPR™ PCSR.

30 Due to the extent of specific items required to address Action A1, EDF and AREVA further split this into sub-actions for convenience as follows:

- A1.1 – substantiation of Type A and B HFEs.
- A1.2 – substantiation of Type C HFEs.
- A1.3 – provision of holistic arguments and evidence for key elements of the proposed UK EPR™ operation.
- A1.4 – provision of analytical evidence on how the design of the UK EPR™ prevents and mitigates violation potential.

31 The resolution plan for both main actions (A1 and A2) included submission of interim deliverables giving details of proposed methodologies and assessments to assist ONR's process. Consolidated key submissions then presented the resulting total submissions for each sub-action. Annex 1 provides details of the key submissions that ultimately form the HF safety case to address **GI-UKEPR-HF-01**.

32 An overview of the submissions for each of the GDA Issue actions is provided within this section. It is important to note that this information is supplementary to that provided within the March 2011 PCSR (Ref. 12) which has already been subject to assessment during earlier stages of GDA. It is also important to note that the deliverables are not intended to provide the complete safety case for HF. Rather they form further detailed arguments and evidence to supplement those already provided during earlier steps within the GDA process.

3.2 GI-UKPER-HF-01 Action A1 Submissions

33 The submissions provided against Action 1 of **GI-UKEPR-HF-01** form the bulk of the material provided by EDF and AREVA during the GDA Close-out stage. It is this work to identify and substantiate the human contribution to the safe operation of the UK EPR™ that seeks to close the gap in analysis that was identified by my assessment at GDA Step 4.

3.2.1 A1.1 – Substantiation of Type A and B Human Failure Events

34 EDF and AREVA's approach to the substantiation of Type A and B HFEs aligned with the general approach stated in section 3.1 above. The first deliverable in this area was the provision of a methodology for the identification and substantiation activity (Ref. 17).

35 This methodology was different to that employed for the GDA Step 4 example analysis as both EDF and AREVA, and ONR had considered the initial method was inappropriate for further use in GDA (Ref. 7). This new methodology was equipment focussed with initial identification activity (using the Probabilistic Safety Assessment (PSA)) seeking to pick out items of equipment (and their associated failure modes) that were risk significant within the PSA. This initial analysis sought to identify the typical maintenance, testing and calibration tasks for the relevant equipment types. This identification process was

undertaken for both "legacy[1]" and "non-legacy" equipment using data sourced from industry to inform what tasks were relevant for "legacy" or typical equipment and gathering opinion from Subject Matter Experts (SMEs) for novel "non-legacy" equipment. Further refinement was undertaken to specify critical tasks by identifying those tasks where an error or violation could result in the failure modes identified previously. The final step in the process was to subject the identified critical tasks to detailed analysis, again with the assistance of SMEs, via a "Human HAZOP" study. This activity identified specific errors and violations associated with the tasks and explored what measures were in place, or needed further consideration, to prevent or mitigate them.

36 Subsequent deliverables to address sub action A1.1 (see Annex 1) provided the results of the earlier stages of the methodology outlined above. These were followed by additional reports that recorded the analyses and substantive conclusions generated by the "Human HAZOP" sessions were developed.

37 In addition to the main body of work to address Type A and B HFEs identified via the PSA a number of associated analytical activities were undertaken. These focussed on areas where HF concerns were apparent in the GDA Issues of other technical disciplines; namely Fault Studies and Internal Hazards. Following earlier presentation of a tailored methodology, two analyses were presented on the human contribution (both via latent failures following maintenance and as initiators) to potential dropped loads scenarios using the Polar Crane and the Refuelling Machine. While separate in their exact approach the methodology taken for these analyses remained risk informed by the severity of the potential fault. Similarly a specific methodology and deliverable addressed the contribution of operators to faults involving Heterogeneous Boron Dilution. This again, whilst different in its exact approach when compared to the overall Type A and B analyses, was fundamentally risk informed.

3.2.2 A1.2 – Substantiation of Type C Human Failure Events

38 The analysis of Type C HFEs was the most extensive area of analysis undertaken during the Close-out of **GI-UKEPR-HF-01**. This reflected the nature of the gap in supporting substantiation identified at GDA Step 4. The methodology applied for the analysis of Type C HFEs during the Close-out stage was the same as that previously used during GDA Step 4 (readers are referred to the GDA Step 4 HF Assessment Report (Ref. 7) for information). As a result, the first deliverables were an updated listing of the Type C claims arising from the PSA, identifying those that would be analysed based on their risk contribution and a schedule of when they would be analysed.

39 Subsequent deliverables provided the analyses of those identified HBSCs. Within these deliverables specific aspects were considered alongside the more general analyses arising from identified PSA claims. The specific analyses were provided to ensure that novel aspects of the UK EPR™ design were explored (e.g. the Non Computerised Safety System (NCSS) and Operating Strategy for Severe Accidents (OSSA)) and to support the assessment of other technical disciplines (i.e. consideration of operator responses to internal flooding and Steam Generator Tube Rupture (SGTR)).

[1] Legacy equipment is that which is identical or very similar to common equipment on existing nuclear power plants (NPPs)

3.2.3 A1.3 - Provision of Holistic arguments and evidence for key elements of the proposed UK EPR™ operation

40 Holistic arguments were provided by EDF and AREVA for particular aspects of the operation of the UK EPR™ in response to this sub action. These deliverables sought to provide overarching arguments and evidence to justify the suitability of the design against concerns identified by ONR during GDA Step 4. The two areas of concern were the adequacy of the UK EPR™ to prevent misdiagnosis of faults and the suitability of the means of transfer between the Process Information and Control System (PICS) and Safety Information and Control System (SICS) in the case of a fault. The evidence provided at GDA Step 4 was deemed by ONR not to have addressed these aspects specifically.

41 EDF and AREVA's approach was to outline the general arguments about the design and its intended operation that address these two concerns. These arguments have then been supported by relevant evidence from other work undertaken during the design of the UK EPR™ both generally and from the specific analyses provided for the Close-out of **GI-UKEPR-HF-01**.

3.2.4 A1.4 – Provision of analytical evidence on how the design of the UK EPR™ prevents and mitigates violation potential

42 Work to identify and substantiate how the design of the UK EPR™ prevents and mitigates violating acts was incorporated into work to identify and substantiate HBSCs and in the presentation of holistic arguments. Analytical techniques such as the Human Hazard and Operability studies (HAZOP) used by EDF and AREVA to investigate Type C HBSCs sought to establish both potential human errors and violations and the means by which the design prevents and/or protects against them. As such the submissions considering violations are those as summarised in sections 3.2.1 – 3.2.3 above.

3.3 GI-UKPER-HF-01 Action A2 Submissions

43 **GI-UKEPR-HF-01 Action 2** requires the provision of a consolidated HF safety case and PCSR update for the UK EPR™ that matches UK expectations. The need for this action was both to better present the claims, arguments and evidence for HF within the UK EPR™ design and to accommodate the newly developed work from the GDA Close-out stage.

44 To address the action EDF and AREVA significantly revised PCSR chapter 18 for HF. This is a substantial change from that previously provided; particularly Chapter 18.1 which is the main presentation of the HF safety case. To develop confidence in their approach to the redevelopment of the PCSR chapter EDF and AREVA provided me with early sight of the proposed structure and its associated justification. This was followed later by a draft submission of the chapter to enable ONR to provide comment and clarification queries prior to its final issue.

45 The new PCSR chapter is presented in a structure that provides the Claims, Arguments and Evidence related to HF in the design of the UK EPR™; a definite departure from the previous iteration. This has been achieved by identifying the basis for safety for HF which is that the risks associated with nuclear safety have been minimised to an ALARP level at the GDA phase. It outlines the key claims and arguments as to how reliable human performance has been ensured, and risks arising from human errors minimised at GDA. Finally it presents the evidence to support these claims and arguments by way of the substantiation of particular HBSCs both pre and post fault.

46 The revision of Chapter 18 also identified clearly where HF had influence on or was influenced by other areas of the PCSR. This has resulted in more evident integration of HF throughout the PCSR with reference to and consideration in other chapters. Consequently, where appropriate, additional changes to other chapters of the PCSR have been made to reflect the changed HF safety case.

4 ONR ASSESSMENT

47 This section presents my assessment of EDF and AREVA's submissions to address each action of the GDA issue on HF **GI-UKEPR-HF01**. These submissions were identified by EDF and AREVA in their Resolution Plan (Ref. 8) provided at the end of GDA Step 4 following discussions with myself on the expectations for Close-out of the HF issue.

48 This assessment has been carried out in accordance with the ONR document HOW2 PI/FWD – Issue 3 (Ref. 1).

4.1 Scope of Assessment Undertaken

49 The scope of the assessment has been to consider the expectations detailed in the GDA Issue, **GI-UKEPR-HF-01**, and the associated GDA Issue Actions. These are shown within Annex 3 of this report. The key requirements, as defined by **GI-UKEPR-HF-01**, are:

- Completion of the identification of Type A HFEs and substantiate the Type A and B HFEs.
  - Complete the identification of Type A HFEs.
  - Substantiate the identified Type A HFEs on the basis of system's contribution to overall risk, and proportionate contribution of human error to its unavailability.
  - Substantiate the identified Type B HFEs.
- Substantiation of the Type C HFEs.
  - Identify additional human based safety claims arising from safety analysis undertaken in response to GDA Issues in related technical areas.
  - Provide a targeted and proportionate substantiation of identified human actions.
- Provision of holistic arguments for key elements of the proposed UK EPR™ operation.
  - Provide arguments and evidence to support the claim that the SOA and Automatic Diagnosis (AD) reduces misdiagnosis potential.
  - Provide arguments and evidence relating to situations with failed AD.
  - Consider whether other holistic arguments / evidence are required to support the safety case for HF.
- Provision of analytical evidence on how the design of the UK EPR™ prevents and mitigates violation potential.
  - Submit a methodology for the substantiation of Type A and Type B HFEs that accommodates consideration of violation potential.
  - Provide additional evidence on how the UK EPR™ design prevents / mitigates violation potential.
- Submission of a consolidated HF safety case and PCSR update for the UK EPR™.

50 The scope of this assessment is both to complete the detailed assessment of the HFE substantiations of the arguments and evidence provided by EDF and AREVA; and to undertake a review of the revised presentation of the HF safety case within the PCSR. There is no intention to undertake further assessment of aspects dealt with in my GDA Step 4 report.

51 I have presented the various parts of my assessments as follows:

- Section 4.2 - the Type A and B HFEs.
- Section 4.3 - the main Type C HFEs.
- Section 4.4 - claims supporting the closure of other GDA Issues.
- Section 4.5 - holistic arguments and evidence.
- Section 4.6 - violations prevention and mitigation.
- Section 4.7 - consideration HF Issues and Assumptions registers.

4.2 Assessment of Type A & B Human Failure Events

52 EDF and AREVA developed a methodology for the assessment of Type A HFEs and undertook an assessment at GDA Step 4 (Ref. 18). Both EDF and AREVA, and ONR jointly judged that the GDA Step 4 methodology was disproportionate in the resources required to perform the assessments for the limited insights it provided. Consequently EDF and AREVA developed a revised methodology (Ref 17) to complete the identification of Type A and B HFEs based on experience of the methodology presented in GDA Step 4. The main elements of this revised methodology are:

- Selection of the most risk significant safety systems determined from the PSA – the systems selection using the same criteria as for the risk significant Type C HFEs; Risk Increase Factor (RIF>2) & Fussel-Vesely (FV>$5x10^{-3}$)[2].
- Primary consideration given to Preventative Maintenance (PM), periodic testing, calibrations – EDF and AREVA argue that any breakdown maintenance is likely to be conducted in a similar manner to PM activities.
- Determination of the risk important equipments & failure modes from the selected safety systems.
- The use of a legacy/non-legacy equipment classification – legacy equipment being that which is identical or very similar to common equipment on existing NPPs.
- Grouping of risk significant equipments by type - to facilitate analysis by type.
- Use of Institute of Nuclear Power Operations (INPO) guidance and a major Electric Power Research Institute (EPRI) database on maintenance strategies & good PM practices (Refs. 19-21) – to facilitate identification of PM tasks, testing & calibration activities; & potential error defences.
- Identification of critical tasks with the potential to introduce significant errors.
- Use of a Human HAZOP workshop for each equipment grouping using SMEs to review critical tasks, identify significant errors and potential control measures.

[2] This is the same risk screening approach as used and assessed at Step 4.

53 The Human HAZOP uses a checklist that includes consideration of violations and the use of the HF Issues Register (HFIR) to record key issues arising from the analyses. The workshops composition includes both HF specialists and equipment and maintenance specialists (from EDF and AREVA).

54 In my assessment of EDF and AREVA's draft methodology I commented that the approach appeared satisfactory for risk proportionate identification of Type A HFEs but that it only partially addressed identification of additional Type B HFEs to the five explicitly identified at GDA Step 4. In response EDF and AREVA state that it has used 3 sources to determine Type B HFEs:

- Analysis of operational experience.
- Studies of specific safety case issues (e.g. dropped loads, heterogeneous boron dilution faults).
- The consideration of maintenance, testing and calibrations tasks on safety significant equipment (via the Type A studies).

55 EDF and AREVA consider that these studies are likely to identify the most significant Type B HFEs – and that the lack of detailed design information available at this point makes further systematic identification difficult.

56 My assessment of this approach has been based both on my detailed assessment of the methodology when presented; and consideration of its application in the Type A/B submissions provided (see below).

57 The main challenge EDF and AREVA have stated they face in identification of Type A and B HFEs is the lack of detailed design and operational information available at this stage of the project; and I accept that this does limit what can be reasonably undertaken for GDA.

58 For Type A HFEs I judge that the methodology has been soundly based on good practices and that the selection and screening approaches focus on those areas that are most risk significant (the same basic criteria have been used as agreed for Type C HFEs at GDA Step 4). I consider that the Human HAZOP approach using SMEs has the capability of combining operational experience (via SMEs) and systematic task and error identification in a resource efficient manner. Additionally I consider the use of the EPRI database is useful as it ensures that world-wide good practices and potential defences have been considered in EDF and AREVA's approach.

59 For further identification of Type B HFEs, I consider that the methodology has limited value as it only focuses on a limited number of safety systems. Human errors with the potential to induce or contribute to an initiating event are more likely to occur when operating or testing plant – particularly in plant states that have the greatest level of human activity (e.g. shutdown states).

60 However I judge that a rigorous, systematic error identification approach for Type B HFEs would be extremely resource intensive and would be of limited value at this point, given the lack of detailed design and operational information available. EDF and AREVA have used operational experience in its initial identification of Type B HFEs at GDA Step 4. The additional studies it cites do give further opportunities to identify significant Type B HFEs.

61 I consider that EDF and AREVA could have undertaken some additional studies in the earlier phases of the work for consideration at the Step 4 assessment – particularly consideration of those operations more likely to generate significant Type B HFEs (e.g.

shutdown operations). However I judge that use of operational experience at GDA Step 4 as part of the initiating event frequency determinations combined with the additional Type A/B identification studies for the GDA Issue close-out is sufficient at this point to ensure that the HF contributions to risk have been included within the PSA risk estimation.

62 I have considered two key factors in making this judgement:

- Discussions with my PSA colleagues at GDA Step 4 indicated that the overall Fault Schedule and Initiation Fault frequencies were soundly based and supported by considerable use of operational experience – hence largely includes human error contributions to risk.
- The detailed design development work that needs to be undertaken by a future licensee includes consideration of AFs (notably AFs **AF-UKEPR-HF- 23, 26 and 31**) from my GDA Step 4 assessment. These AFs include measures to consider and reduce human error at both system and equipment design levels. These measures encompass both Type A and B HFEs and will help to ensure that the contribution from Type A and B HFEs is As Low As is Reasonably Practicable (ALARP).

Identification & substantiation of Type A HFEs – additional details

63 Although the approach has not considered all potential Type A HFEs, I judge that sufficient has been done to adequately complete identification of risk significant Type A HFEs for GDA.

64 EDF and AREVA conducted HAZOPs for the following equipment types:

- valves;
- pumps, electric motors, low pressure tanks, heat exchangers.
- Sensors, electrical systems; and
- control and instrumentation (C&I) without sensors, Reactor Coolant Pump (RCP) seals, chiller units, Diesel Generators (DG).

65 These studies have identified a combination of means that may be used to reduce the likelihood of, or eliminate HFEs that were been identified from operational and maintenance activities. These defences included:

- design measures;
- passive safety measures (e.g. using size/shape/geometry to prevent mis-connections);
- active engineered safety measures (e.g. alarms on detection of incorrect equipment state); and
- operational practices and administrative controls.

66 The analyses have produced 76 individual HFIR items that encompass the equipment specific HFE reduction or prevention measures identified.

67 My assessment of these analyses is that they have been thorough and have identified potentially useful means of error prevention. I consider that the error reduction and prevention measures identified appear to be appropriate and potentially provide useful means of ensuring that the detailed designs are ALARP. However I note that the studies have not been able to consider the practicalities of implementing any specific measure for a specific component in a given safety system. The practicability and merit of each

measure will need to be considered against other design requirements and constraints when the detailed system and equipment designs are developed post-GDA.

68 I have raised a general Assessment Finding on further consideration/implementation of identified HFIR items in section 4.7. This will encompass the HFIR items and recommendations arising from the Type A HFE analyses.

Identification & substantiation of Type B HFEs – additional details

69 EDF and AREVA's consideration of Type B HFEs during GDA closure has been:

- Via the potential identification of additional Type B HFEs during the consideration of Type A HFEs.
- Provision of EDF existing fleet operational experience to provide justification of five Type B HFEs that had been identified for GDA Step 4.

70 The Type A analyses have not identified any additional Type B HFEs. However I judge that the recommendations for error reduction or prevention identified from the Type A analyses related to each equipment grouping may help to reduce the potential for Type B HFEs in some systems and for certain operations.[3]

71 I consider that the operational experience evidence presented indicates that EDF has established formal processes to capture operational experience systematically and to use it in the design of EPR™ designs including the UK EPR™. I judge that this Operational Experience (OpEx) has enabled the incorporation of useful fault prevention measures into the UK EPR™ design. I also consider that the evidence presented is sufficient to underpin the assumed initiating fault frequencies for the five previously identified Type B HFEs. These are:

- homogeneous boron dilution events during at-power and shutdown states;
- uncontrolled level drop during shutdown state Cb;
- fire in the MCR during at-power states;
- flooding in turbine building during at-power states; and
- flooding in safeguard building during at-power states.

72 However the evidence presented is insufficient to verify that the current design is ALARP for Type B HFEs though I consider that EDF and AREVA have done sufficient to substantiate the Type B HFEs to satisfy the GDA Issue action. Further verification of the identification and substantiation of Type B HFEs will need to be undertaken by a future licensee. This is encompassed by **AF-UKEPR-HF-01 and 03** I raised at GDA Step 4 requiring revision of the HRA and inclusion of all relevant Type B HFEs in the Level 1 PSA.

4.2.1 Conclusions for Type A & B Human Failure Event Identification & Substantiation

73 I consider that EDF and AREVA have undertaken considerable analysis in order to complete the identification of both Type A and B HFEs. I judge that their analyses of the most risk significant safety systems has been sufficient to identify the most likely

[3] This is as these recommendations are general error reduction/prevention measures – consequently some 'defended' errors may have had the potential to lead to Type A and/or B HFEs. The measures do not differentiate between the differing types of HFE.

significant Type A HFEs, as far as this is possible at this stage of the design development.

74 I judge that EDF and AREVA have done limited additional work that is capable of further identification of Type B (initiator) HFEs. However I acknowledge the arguments made by EDF and AREVA that further work at this stage will be of limited benefit due to the lack of detailed design information available. I also consider that **AF-UKEPR-HF-23** on HF requirements for design specifications made at GDA Step 4 will help to ensure that the contribution from both Type A and B HFEs is ALARP.

75 EDF and AREVA have not been able to provide complete qualitative analyses to fully substantiate both the Type A and B HFEs identified at this phase of the project. However I judge that the error barriers and recommendations EDF and AREVA have identified are an important input into ensuring that the design will result in a risk that is ALARP. All of these error barriers have been identified in the HFIR items stemming from these analyses. Consequently these will need to be further considered and implemented by a future licensee as part of its detailed design development work. I have raised a general AF (**AF-UKEPR-HF-60**) on the implementation or consideration of HFIR items in section 4.7 which includes the HFIR items related to Type A and B HFEs. Further useful work requires the detailed design information that will only be available post-GDA. Additionally the detailed design development work should build in error reduction/prevention approaches that will be applicable to both Type A and B HFEs.

76 I consider that a future licensee should undertake further work so that the detailed design specification process accommodates sufficient HF requirements to ensure detailed designs are ALARP for human error during maintenance and operation. It will also need to provide further substantiation on the identification and substantiation of Type A and B HFEs. This will need to consider potential dependencies related to Type A and B HFEs as part of the overall HRA revision. I regard these issues as being part of the expected design and safety case development work that a future licensee will need to undertake post-GDA.

4.3 Assessment of Type C Human Failure Events

4.3.1 Type C Human Failure Event Methodology

77 EDF and AREVA presented a methodology for the substantiation of Type C HFEs along with three examples of its use to substantiate Type C HFEs at GDA Step 4 (Refs. 22 and 23). This methodology, as implemented used a combination of hierarchical, tabular and timeline Task Analysis (TA). I considered the examples presented at GDA Step 4 were of a high standard, and provided a detailed analysis in support of the HBSCs.

78 For the Type C HFE Close-out work EDF and AREVA stated that they would use the same methodology. The level of detail would be tailored according to the risk significance of the Type C claim. The methodology defined high, medium and low risk claims (medium and high risk claims having RIF values >2 and FV >0.005). Medium risk claims are further classified into medium and medium complex; with the latter classification used for claims that have multiple actions or staff involved. EDF and AREA stated that they would provide similarly detailed TAs for all high and medium complex risk' Type C HFEs as for the three examples presented at GDA Step 4; and a reduced level of detail for medium risk claims.

79 The methodology includes the use of 'bounding' assessments where one claim scenario is used to provide the basis for substantiation of other similar claims and/or modified scenarios. I consider this approach to be acceptable as long as the choice of the

bounding claim is appropriately justified and considers the most challenging demands for operator response – not just the most risk significant scenario which may not be the most demanding for operator response.

80 I consider that for the Type C HFEs EDF and AREVA have maintained the quality of submissions with similar levels of detail. I note that detailed TAs have generally been provided for medium level claims.

81 I consider that there have been some notable changes from the first examples that have had an impact on the degree of substantiation provided. These changes have been:

- The increase in assumptions used – due to the lack of detailed information on systems, procedures and operational details.
- Reduced use of the EPR™ simulator – due to limitations in the simulator modelling or addressing certain tasks (e.g. local to plant; Non-Computerised Safety System (NCSS) actions).
- Increased reliance on SMEs to provide judgements on envisaged operational practices based on operational experience.
- Reduced level of detailed analysis for transfer to, and operation of NCSS tasks – due to the limited information on the NCSS arising from its early state of design development.

82 Where the changes described in the previous paragraph have arisen, I consider that EDF and AREVA have taken reasonable steps to ensure that the TAs have provided an appropriate level of analysis. For example ensuring that sufficient appropriate SMEs have been used to provide information on the most probable operational approaches and times for task executions.

83 The methodology has been complemented by the creation of both a HFIR and HF Assumptions Register (HFAR). These two registers have been developed in response to my comments on draft assessments to ensure that all key findings and assumptions from the substantiations have been recorded for a future licensee to consider and/or implement. The HFIR and HFAR have been used to record all findings and assumptions from all the HF work undertaken during the GDA Close-out programme. I comment on them further in section 4.7 below.

84 Overall, I judge that the Type C HFE assessment methodology is appropriate, and based on good practices that are consistent with ONR's SAP and TAG expectations. Its implementation has been of high quality and has provided as much insight into the claims as could reasonably be expected at this phase of the project.

4.3.2 Substantiation of Type C HFEs

85 My assessment of the Type C HFEs has focussed on those areas of potential significance to safe operation of the UK EPR™ using insights from the PSA results to aid my judgement. I have considered areas of inherent uncertainty and on key activities that support several important discrete claims. The notable areas have included:

- Claims for NCSS operator actions – requiring transfer from the main PICS interface to the SICS panels and enabling of NCSS.
- All high risk claims.

- Key Level 2 PSA claims when severe accident conditions arise; and the operators have to exit SOA operation and start using OSSA strategies and severe accident procedures.
- Actions requiring local to plant actions.
- Claims to support resolution of other GDA Issues – see section 4.4.

86 My assessment of the post-fault Type C HFEs examples at GDA Step 4 identified an issue on the adequacy of the HMI and supporting procedures for monitoring some tasks (lack of trend & rate displays at the main overview display level and on provision of suitably compelling cues for operator actions). This has been an area I have continued to examine in my assessments.[4]

87 EDF and AREVA have provided 12 individual Type C HFE substantiation reports (see reports listed for D2.5 in Annex 1). These include revision of the examples provided at GDA Step 4 to respond to the comments I made on the substantiations in my GDA Step 4 report (Ref. 7). These HF analyses typically consider one, or a small number of bounding HBSCs that potentially underpin additional ones that are modelled in the Level 1 or Level 2 PSA.

88 Annex 4 provides individual summaries of the detailed assessments I have undertaken of these Type C submissions. I have considered how far the current claims have been substantiated; how well issues and assumptions that need to be further addressed have been identified; and on the acceptability of reliance on operator action for the claims made. Where 'bounding' scenarios or claims have been used to support several claims or differing scenarios I have considered how well the selected bounding claim supports the others.

89 I have assessed all the Type C submissions provided by EDF and AREVA. From these assessments I conclude that:

- All medium to high risk HBSCs have been encompassed by the detailed TAs provided.
- The substantiations are generally detailed task analyses that do consider all key influencing factors.
- Some of the substantiations are necessarily limited due to the phase of design and the consequent lack of detailed procedures.
- The HFIR and HFAR have adequately captured all key findings and assumptions that need to be considered further or implemented by a future licensee.
- No further consideration of the low risk claims has been made by EDF and AREVA; their consideration is covered by GDA Step 4 HRA work.

90 I note that all of the Type C substantiations have been based on the FA3 operating staff roles (Ref. 24), HMI (including use of the AD and procedures (SOA), Manual Operating Procedures (MOP) and OSSA as at GDA Step 4. Consequently these roles form an important aspect of the HF safety case. A future licensee will need to ensure that the assumptions and requirements stemming from the use of the FA3 operating philosophy are maintained or revised justifications provided for any changes made. I regard this as

4 The MCR HMIs and simulator allow a more detailed examination of the Type C HFEs. For Type A and Bs they require more information about the discrete equipment and operating/maintenance procedures that have not been determined.

fundamentally underpinning nearly all the HF safety case presented at GDA consequently I have raised the following AF.

> ***AF-UKEPR-HF-55:*** *The Licensee shall ensure that its operating philosophy is consistent with the assumptions made in the GDA HF substantiations on the use of the SOA approach, procedures, and on the key operating roles of Action and Strategy Operators (OA and OS) and the Safety Engineer (SE). If an alternative approach is intended by the licensee then re-justification of all relevant HBSCs will be required and re-analysis as necessary.*
>
> **Required timescale:** Prior to First structural concrete.

91 Many of the Type C analyses have identified the need for enhanced HMI provisions to support reliable monitoring of safety functions. This includes consideration of:

- The provision of additional trend and rate information within the HMI at the display level normally used for SOA implementation to assist the operators' awareness of the speed of scenario developments.
- The need for sufficiently compelling cues to prompt timely operator response.
- The inclusion of additional specific parameter displays.

92 I note from my assessments that these have been identified in the discrete HFIR entries from each TA. As the claims are likely to be revised as the safety case develops post-GDA, I regard this as an important area that a future licensee needs to pay particular attention to in the development of the HMI for the UK EPR.

93 Additionally I note that in some cases specific details need to be incorporated into SOA procedures and/or MOPs to ensure that operators are alerted to particular plant status and guidance to perform a specific task. The HFIR entries have included identification of such procedural issues. I consider that all the identified HFIR items are appropriate but further consideration or implementation of them will need to be undertaken by a future licensee as part of the more detailed site specific design. I have raised an AF finding on the HFIR items in section 4.7 that encompasses this requirement.

94 There has been one additional item that I judge to be important from my assessment of the Type C submission that has not been included in HFIR items. This is for loss of C&I scenarios (claim H4, OP_EFWS and for NCSS claims) where further determination of the credible degradation or failure of the C&I (notably the Teleperm XS (TXS) system) that will impact the PICS displays and consequently affect the operator responses.

95 Generally I consider that PICS failures are likely to be readily detected (e.g. there are in-built features flagging up failed or incorrect individual inputs) however I consider that the detailed determination of the impact of C&I failure modes on the PICS displays and hence operator responses is very important and requires consideration by a future licensee. In consequence I have raised an AF on this.

> ***AF-UKEPR-HF-56:*** *The Licensee shall determine the impact of credible degradation and failure modes of the C&I systems on the PICS displays and their resulting impact on any claimed operator actions. The licensee will need to re-substantiate any affected HBSCs.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*
>
> .

96 Several of the substantiations have identified that an alarm provides a potential cue to alert the operator to the need for a response, and indicated that the alarm needs to be appropriately classified. The need for consideration of alarms is included in the HFIR items raised by EDF and AREVA. From my GDA Step 4 assessment I consider that further consideration of the use of alarms during SOA operation is required to ensure reliance on alarms as a cue for timely operator actions is valid. EDF and AREVA at GDA Step 4 indicated that once SOA operation is entered then the operators are not required to respond directly to any discrete alarms other than the AD re-announcing unless directed explicitly by a procedure. It is also likely that all alarm sounds apart from the AD will be muted at least in the early phase of an emergency response hence making their alarming less compelling.

97 I consider that alarms potentially do provide very useful information to the operators during SOA operation. From my assessments I consider that the monitoring of alarms during SOA operation, accompanied by procedural guidance could provide important support to timely operator responses. The use of the Plant Overview Panel (POP) appears to offer potential to provide enhanced alarm information. At GDA Step 4 I raised two related AFs to this issue:

> ***AF-UKEPR-HF-46 –*** *The licensee shall include a permanent display of active alarms in the UK EPR™ MCR alarm design specification, or justify why this is not required.*
>
> ***AF-UKEPR-HF-38 –*** *The licensee shall ensure that the information presented to the operators supports situation awareness. Should a POP be proposed for the UK EPR, consideration should be given to dedicated formats.*

98 Reliance on, and monitoring of alarms when used as compelling cues during SOA operation needs further consideration by a future licensee both to support discrete claims and to ensure a coherent emergency response approach in the reliance on, and response to alarms during SOA operation.

> ***AF-UKEPR-HF-57:*** *The Licensee shall determine the most effective use and presentation of alarms to support claimed operator actions during SOA and OSSA operations. This shall include consideration of the use of the Plant Overview Panels as a means of displaying alarms and how any specific alarm monitoring should be included in SOA operation by both the OA, OS team and the SE.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*

Non-Computerised Safety System Operation

99 The Type C HFEs include several claims (one high risk claim H8 and five medium risk claims M9, 10, 11, 13, 18) that require transfer from the PICS workstations to the NCSS HMI which is a part of the SICS panel. These claims are required for scenarios with combined PICS and SICS failures that are modelled as failure of digital C&I in the PSA.

100 From the operator perspective these claims are similar to scenarios with C&I failures requiring transfer to the SICS panel (see section 4.5.2). I judge that the key challenges for such tasks are most likely to be:

- The recognition of loss of the SPPA-T2000 and TXS C&I digital systems (i.e. PICS and SICS failure) and diagnosis for the need to transfer to NCSS operation.
- The transfer and initial re-orientation for operation from the NCSS.

101 As the details of the SICS panels and particularly the NCSS design are not fully determined, much of the substantiation offered has relied on assumptions on both design details and supporting procedures. I consider that all of these assumptions appear reasonable but will need to be implemented by a future licensee or alternative justification provided.

102 My assessment of the NCSS claims analyses has not identified anything in principle which would indicate that reliable operation and achievement of each claim cannot be achieved once transfer to NCSS has been undertaken. The only significant issue that I have noted is the likely time required to recognise and achieve transfer from the PICS to NCSS. For situations with rapid total failure of PICS and SICS then I judge that the recognition and transfer will be both quick and reliable. EDF and AREVA have provided operational experience that supports this view from N4 training exercises for loss of C&I scenarios.

103 I do not consider that at this point EDF and AREVA have provided sufficient evidence on the consideration of the range of credible failure modes of the PICS systems, particularly for progressive degradation. I have raised Assessment Finding **AF-UKEPR-HF-56** on this (see above).

104 Following discussions with my C&I colleagues, overall I am satisfied that the claims currently being made for NCSS actions can be adequately supported with the appropriate detailed design and supporting procedures. These HF claims are relatively modest and the capability and reliability of the NCSS system should readily support the claims. This matter will need to be progressed by a future licensee as part of the normal design and safety case development for the NCSS and associated operator actions.

OSSA entry and actions

105 Monitoring the OSSA entry criteria is currently assumed to be the responsibility of the SE. This is normally recognised by high Core Outlet Temperature (CoT) reaching 650^0C, or in circumstances when this parameter is not available (primarily shutdown conditions) on high containment dose rate the latter of which requires calculation by the SE and comparison with a table to determine the dose rate values after any given time after shutdown.

106 The EDF and AREVA analysis has identified that recognition of OSSA entry criteria is not simple. It has identified HFIR items that would enhance the reliability of recognition of OSSA entry criteria for both parameters (see Annex 4). I consider that these HFIR items need to be addressed by a future licensee post-GDA along with further consideration as to how the OA and OS can support reliable OSSA entry by monitoring PICS parameters.

107 In my assessment of the OSSA entry and actions (see Annex 4 for claims M21, 22 & 24[5]) I noted that the analysis assumes that entry into OSSA procedure and actions is dependent on the SE contacting the Emergency Director (ED) who is potentially off-site; and for the ED taking the decision to enter OSSA. The time estimated by the task analyses to contact the ED and make the decision is taken as 17 minutes[6]. The SE has the responsibility for determining that OSSA entry criteria have been met.

[5] *EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims Primary circuit depressurisation in the EOP and the OSSA*

[6] Contacting the ED is only one part of the overall claimed actions and the overall time for the claimed actions is far longer with potentially acceptable margins.

108 I can envisage exceptional situations where it may take longer to contact the ED. Additionally the ED has no additional information to use in order to determine whether OSSA entry is appropriate. I consider that it appears preferable for the decision to enter OSSA procedures to be taken by the SE – perhaps confirmed by the SS – and the ED to be contacted to consult on the overall OSSA strategy to be implemented. This would ensure that no immediate OSSA actions were delayed (e.g. primary circuit depressurisation; containment isolation) unnecessarily. I recommend a future licensee to review the OSSA arrangements to ensure that key immediate actions are not unnecessarily delayed. I have not raised an AF on this as it does not impact on the safety case at the GDA stage.

Operating Roles & Procedures

109 The Type C substantiations are all reliant on the assumed operating philosophy for FA3 with five main roles identified and on the SOA approach. The five main roles are:

- An OA – who implements the detailed SOA and MOP instructions.
- An OS – who maintains an oversight of the SOA.
- The SE – who is called in when SOA operation is entered and monitors key safety functions from the SICS panel.
- The SS – who undertakes the SE's role during SOA operation until the SE arrives.
- Field Operators (FO) who undertake local to plant actions required post-fault.

110 The MCR staff use a combination of paper and computer presented procedures. The SOA procedures are paper based with different versions for OA, OS and SE. The OA and OS will also have different paper based SOA procedures for SICS and NCSS operation.

111 I consider that the Type C substantiations, including those supporting other GDA Issues (see section 4.4) are very reliant on the roles assumed within the analyses, and on many key aspects of the procedures. I discuss several key aspects further in section 4.5.1. I judge that the HF substantiations are dependent on four of the five key roles. I consider that the SS role is not substantive other than when performing the SE role prior to the SE's arrival in the MCR.

112 In consequence I judge that the GDA HF safety case is highly reliant on the assumed roles for OA, OS, SE and FO (where relevant) and operating approaches. A future licensee will need to implement these arrangements or provide a detailed justification of all relevant HBSC claims based on an alternative approach.

> ***AF-UKEPR-HF-55:*** *The Licensee shall ensure that its operating philosophy is consistent with the assumptions made in the GDA HF substantiations on the use of the SOA approach, procedures, and on the key operating roles of Action and Strategy Operators (OA and OS) the Safety Engineer (SE), and Field Operator (FO). If an alternative approach is intended by the licensee, then justification and re-analysis of all relevant HBSCs will be required.*
>
> **Required timescale:** Prior to First structural concrete.

4.3.3 Conclusions for Type C Substantiations

113 EDF and AREVA have provided detailed substantiations for all significant Type C HFEs.

114 I consider that only a very small number of Type C HBSCs have been fully substantiated and that most are partially substantiated. For most of the partial substantiations I judge that a valid claim appears to be potentially supported – the identified HFIR issues and key

assumptions need to be appropriately addressed or implemented by a future licensee in order to support a valid claim.

115 I consider that the Type C substantiation work identifies several key areas that need to be considered both for the specific claims and more broadly in the future detailed design phase. These are:

- HMI Displays – there are three main areas that have been identified:
  i) The provision of unambiguous compelling cues to operators to take key actions.
  ii) Ensuring that trend and rate information is provided at an appropriate display level to ensure operators are aware of the progression of scenarios.
  iii) Ensuring that alarms used to alert operators to key actions are appropriately categorised, and compelling for operators to respond to on the timescale required.
- SOA and computerised procedures – the analyses indicate that for some claims the details (e.g. sequencing, specific instruction, systematic checking of plant state) are important to ensure claimed actions are reliable and undertaken within the necessary timescales.
- Alarm response philosophy.
- Transfer from PICS to SICS interfaces (for both SICS and NCSS operation).

116 There are a few claims I judge to require more detailed substantiation. For most of these claims I judge that it is likely that a valid claim can be supported if the associated HFIR items are addressed, or that recommended revised transient analysis removes the need for the claim or extends the timescale. These claims need to be considered by a future licensee to determine if a claim on operator actions can be made, and if not then ensure that an acceptable alternative position is justified to support an ALARP position. I judge that the risk impact of these not fully substantiated claims is likely to be relatively small on the overall PSA assessed risk for the UK EPR™ due to their small number and relatively low individual risk contributions.

117 Overall EDF and AREVA have done sufficient work to meet the requirements of this part of the GDA Issue. Further work is required to provide full substantiations for all claims but the analyses have gone as far as is reasonable at this point in design & safety case development. This provides further confidence that an acceptable position for all operator action claims can be ensured.

4.4 Assessment of Operator Action claims supporting other GDA Issues

118 This section provides additional commentary on my assessment of operator action claims or HFEs that support closure of other GDA Issues. Four issues include reliance on key claims for operator actions or consideration of significant HFEs. These are:

- Dropped loads; **GI-UKEPR-IH-01** (Ref. 26)
- Internal Flooding; **GI-UKEPR-IH-03** (Ref. 27) and (Ref. 33)
- Heterogeneous Boron Dilution safety case; **GI-UKEPR-FS-01** (Ref. 28)
- Steam Generator Tube Rupture safety case; **GI-UKEPR-FS-04** (Ref. 29)

119 Additionally **GI-UKEPR-FS-02** on diversity for frequent faults may result in some claims on operator actions. I have consulted with my fault studies colleague and at this point no claims have been identified that have required substantiation. However it is likely that

some of the AFs arising from Close-out of the issue could lead to the identification of new HBSCs. These will need to be addressed by a future licensee.

4.4.1 Dropped Loads

120 Annex 5 provides a summary of my detailed assessment of the HF submission on HBSCs arising from the Dropped Loads safety case. These analyses present the identification of the potential human errors contributing to dropped loads and any potential recovery actions. They also consider the levels of defence provided, or anticipated, and the potential adequacy of the position. They are not intended to be full substantiations for the HBSCs but to indicate whether the claims appear reasonable at this point and whether it is judged that additional defences are likely to ensure an ALARP position.

121 EDF and AREVA have provided two analyses; one for representative activities involving the refuelling machine and the other for movements of the reactor cavity slabs using the main polar crane. These analyses have identified:

- For the Refuelling machine - one direct human error leading to disengagement of gripper during horizontal movement.
- For the Polar crane – seven human errors contributing to key slab drops; four potential recovery actions.

122 For each HFE the level of defence has been considered and generic defences identified. The overall recommendations stemming from these analyses are for a future licensee to implement the identified defences.

123 My assessment of these dropped load HF analyses is that EDF and AREVA have implemented the agreed approach for consideration of the HBSCs at this point to support the closure of the Internal Hazards GDA Issue **GI-UKEPR-IH-01**. The analyses have not identified anything that indicates to me that an acceptable position cannot be achieved once the detailed design and procedures have been developed. A future licensee should consider the conclusions and recommendations arising from these reports in further developing the design and supporting dropped loads safety case.

4.4.2 Internal Flooding

124 The GDA Issues and actions relating to Internal Flooding **GI-UKEPR-IH-02** (action A3) and **GI-UKEPR-IH-03** require provision of adequate substantiation of the internal flooding safety case. The safety case provided (Ref. 34) includes claims for operator actions to isolate some leaks. A separate HF submission (Ref. 35) provides consideration of a range of operator actions in response to alarms (sump alarms) following a wide range of leak scenarios in differing buildings:

- Reactor Building (HR A and B).
- Fuel Building (HK).
- Safeguard Buildings (SAB and HL).
- Diesel Buildings (HD).
- Nuclear Auxiliary Building (NAB).

Most of these scenarios then require local to plant actions to isolate the leaks.

125 The HF report covers several claims for manual leak isolation actions for the following:

- HR3 – pipe breaks of several sizes in the Nuclear Island Fire Fighting Water Distribution system (JPI) system located in HRB.

- HR4 – a DN[7] 50mm pipe break in the Demineralised Water Distribution system (SED) system located in HRB.
- HK1 – a DN 50mm pipe break in the Nuclear Island Fire Fighting Water Distribution system (JPI) system located in HK.
- HL2 – a DN 50mm pipe break in the Drinking Water Distribution system (SEP) system; and a large pipe break in the Essential Service Water system (SEC) system both located in the Safeguard building (SAB).
- HD1 – a DN 50mm pipe break in the Diesel Building Fire Fighting Water Distribution system (JPV) system located in HD A.

These claims stem from scenarios that assume that a single primary isolation valve has failed.

126 A more complicated situation arises for very limited cases where isolation of the fire fighting distribution system (JPI/JPV) is required to isolate a leak. This requires operators to confirm that there is no potential fire and demand on the system prior to undertaking the isolation.

127 For medium energy classified pipework with a nominal diameter greater than 50mm the assessment generally only considers pipework breaks with a break area of DT/4[8] – this has an important impact on the assumed times available for leak detection and isolation. It has also included key claims on larger breaks in key scenarios:

- For HRB2 – a DN 150mm break in the Fuel Pool Cooling system (PTR) suction line
- For HL2 – a DN 700 mm break in the SEC

128 I consider that EDF and AREVA have undertaken a detailed TA of MCR and Local to Plant (LTP) operator actions. This includes detailed timeline assessment for the FO journey times to isolation locations using a 1km/hr speed on a Computer Aided Design (CAD) plant model to allow for access & journey elements (doors, stairs, steps etc.). The analyses assume that flooding occurs during normal operation and entry into SOA operation is not required.

129 For most of the scenarios the analyses show that there is a considerable margin between the time needed to undertake the claimed operator actions and that required by the safety case. However there are a small number of cases where either the time required to undertake the actions exceeds the safety case time or there is very little margin. These scenarios are for HR3, HR4 and HRB2c claimed actions.

130 Additionally the analyses generally show:

- Leak detection is apparent for all leaks via high sump alarms
- Determination of the location of the leak is generally more difficult due the lack of clear indication of the leak location; consequently detailed leak response procedures are needed to undertake systematic leak location determination.
- For some scenarios the operators will have to check that the fire fighting system is not required before isolating the JPI system

[7] DN = nominal diameter

[8] DT/4 – where D=nominal diameter; T=thickness

- Automation of some local to plant tasks for HR3 and HR4 scenarios are required to remove the need for some local to plant actions. [9]
- Automation of some leak isolation tasks for HRB2c needs to be considered. [10]
- Manual stopping of the SEC pumps as the primary means of leak isolation for the HL2 scenario needs to be included in the leak response procedure.

131 My assessment of the HF submission (see Appendix 4 for further details) is that it has generally been appropriate and I support the recommendations and HFIR items identified in it. These cover several general issues:

- The procedures need to contain sufficient detailed information for reliable leak detection and response (particularly for systematic leak source identification).
- The HMI lacks specific parameter information to aid the MCR operators in leak response.
- The response times for situations with consequential faults (leading to SOA entry) need to be considered for acceptability.
- For the HR3 & HR4 scenarios motorised valves need to be installed to remove the need for local to plant actions. [11]
- Automation of some leak isolation tasks for HRB2c should be considered. [12]
- The operators determine that there is no fire risk (for JPI isolations) by referring to a dedicated fire alarm panel. If alternative fire risk surveillance methods (e.g. location CCTV) then this may increase the leak isolation times.
- The leak isolation procedures for the HL2 scenario need to identify manual stopping of the SEC pumps as the primary means of leak isolation.

132 From my assessment of the HF submission I judge that a potentially important issue has not been fully addressed. This is confirmation that the internal flooding scenarios do not lead to the generation of other alarms. If other alarms are generated this could mask the relevant leak alarms or lead to delays in response due to the operators having to deal with a more complex situation. The report indicates that this needs to be addressed further post-GDA. I have raised an AF on this.

> ***AF-UKEPR-HF-58:*** *The Licensee shall determine if internal floods generate additional alarms that are likely to mask or delay response to key alarms or indications prompting operators to undertake claimed leak response actions. The licensee shall provide an appropriate justification that any claimed operator actions required to support the Internal Hazards flooding case are reliably achievable within the required timescales.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*

Overall conclusions for Internal Flooding HF submission

[9] These design modifications have since been included in the GDA design

[10] Additional automation has since been included in the GDA design.

[11] These design modifications have since been included in the GDA design

[12] Additional automation has since been included in the GDA design.

133 My overall judgment is that EDF and AREVA have shown that most claims for operator responses to leaks are feasible and should be adequately reliable providing that the identified HFIR issues are addressed for specific HMI and procedural requirements by a future licensee.

134 EDF and AREVA have identified the potential for additional automation to address those operator claims that appear to be insufficiently feasible or reliable. The basis of the case is that credible floods will not lead to situations threatening key safety functions – and that any leak responses required from operators occur before conditions degrade to a significant point requiring SOA operation. These apects, along with consideration of the acceptability of reliance on operator responses in relation to ALARP, is considered further in the Close-out report for **GI-UKEPR-IH-03**. A future licensee will need to consider the overall safety case further. At this point following consultation with my Internal Hazard colleague I judge that EDF and AREVA have provided sufficient information to give confidence that a final acceptable position can be achieved that does not place any unreasonable reliance on operator actions to respond to internal flooding events.

4.4.3 Heterogeneous Boron Dilution

135 The concern raised in the GDA Issue **GI-UKEPR-FS-01** relates to the creation and introduction of a slug of un-borated water into the primary circuit that then causes a reactivity excursion. There are a range of operator actions and errors that are associated with this case:

- Operator errors during maintenance and operations that can create an un-borated source of water.
- Operator errors that can allow transfer of a slug into the primary circuit.
- Pre-fault administrative controls and operational practices that prevent or minimise the likelihood of creating an un-borated water source.
- Operational practices and operator recovery actions that prevent transfer of an un-borated slug into the primary circuit (PC) – these are normally after either sampling boron concentrations or response to alarms.

136 The HF submission (Ref. 32) assesses a set of bounding sequences that stemmed from early Heterogeneous Boron Dilution (HBD) safety case. EDF and AREVA have further developed their HBD safety case and presented a revised case in Ref. 30 supported by a detailed ALARP assessment (Ref. 31). This case has aggregated previously identified sequences into 5 bounding faults (see Table 2 reproduced from Ref. 30 below). It has included a design change to provide an interlock that prevents start up of the no.1 RCP pump until the Chemical and Volume Control System (CVCS) letdown has run for sufficient time (1 hour) to ensure clearance of any un-borated slugs. This provides additional defence against a large range of identified HBD sequences to the administrative and operational controls previously identified. It provides a back-up to the claim for operator action (and associated administrative controls) to undertake RCP start-up in this manner.

137 The Bounding Fault (BF) Initiating Event (IE) frequencies are reliant on the frequencies assumed for each of the individual sequences. Many of these are dependent on Human Error Probabilities (HEP) for key operator actions. Ref. 30 provides details of these HEPs which have been based on using the Human Reliability Analysis (HRA) method used for the GDA Step 4 HRA work described in Chapter 15.1.3.5 of the PCSR. This approach has used assumptions based on notional HEPs. Appendix A of Ref. 30 provides details of

the overall IE frequency for a sequence, the HEPs assumed for claims in the sequence and the calculated IE frequency of a HBD event from each sequence.

138 I note that the final HBD safety case is reliant on a small number of specific HF aspects:

- Reliable operator compliance with procedures for RCP start-up and Residual Heat Removal (RHR) operations to ensure any un-borated slugs are removed (preventative measures if a HBD slug has been created)
- Substantiation that the notional HEPs used in deriving the BF initiating event frequencies are correct or conservative – these HEPs reflect:
  - reliable operator responses to key alarms (primarily boron concentration alarms) to prevent an un-borated slug of significant size being created or transported; and
  - reliable operator sampling of identified water sources (e.g. filled accumulators) and corrective actions on low boron concentration.

139 My assessment of the HF submission has been based on consideration of the wider HBD case, in particular the final position presented in Ref. 3 and insights from Ref. 4. I have consulted with my Fault Studies colleague on the overall HBD case to determine the reliance of it on HF claims.

140 My assessment has focused on:

- The level of substantiation provided by the analyses to support the key HBSCs.
- How well the HF substantiations support the overall HBD case.

141 The HF contribution to the overall case stems from the operator errors and preventative actions claimed as part of the determination of IE frequencies for HBD bounding faults BF1-5.

142 I have assessed each sequence analysis and judge that EDF and AREVA have adequately identified the critical tasks and errors. There has been systematic consideration of the Performance Shaping Factors (PSF) that are likely to be important to the task reliability or error probability. I judge that the findings and recommendations arising from the analyses seem appropriate and have identified the main potential ALARP measures for each scenario.

143 The HF report has not considered each claim against its notional HEP reflected in Ref. 30. However the qualitative analyses performed do provide a sufficient basis to determine whether the notional HEPs are adequately supported – or capable of being achieved if the identified recommendations are implemented.

144 The HBSCs included in the HBD case are for normal or incident operations that would form part of ‘normal operations’ (i.e. not requiring entry into SOA procedures). They are:

- Routine operations or maintenance undertaken during shutdown conditions.
- Sampling actions required as part of a routine surveillance or post-operation.
- Response to alarms (generally boron concentration meters).

145 From the qualitative analyses provided in the HF submission (Ref. 32) I judge that the notional HEPs used in the overall HBD case (Ref. 30) are either supported or readily capable of being achieved providing the recommendations for specific design and procedure features identified in the HF assessment (Ref. 32) are adopted.

Overall conclusions

146 I consider that EDF and AREA have provided adequate HF substantiation of the HBSCs included in the overall HBD safety case (Ref. 32) – provided that the specific design and procedure features identified in the recommendations (and HFIR) are implemented.

147 The main defences that are reliant on operator actions (sampling; response to alarms; undertaking of specified operations) appear to be reasonable and appropriate. The HEPs used appear reasonable and achievable.

148 I judge that this assessment merits an AF indicating that a future licensee should either implement the HFIR recommendations to support the HBD case or provide a justification as to why these are not required to meet ALARP requirements. This AF is included within the Fault Studies GDA Close-out report as it forms a discrete package of requirements stemming from the Heterogeneous Boron Dilution safety case in response to **GI-UKEPR-FS-01**.

4.4.4 Detection and Management of Steam Generator Tube Rupture Faults (SGTR)

149 A GDA Issue **GI-UKEPR-FS-04** was raised relating to the adequacy of the safety case for SGTR. This included Action FS-04.A2 for EDF and AREVA to provide a HF justification of the actions claimed in the design basis safety case for the PCC-3 fault. The related deterministic safety case (Ref. 36) for Steam Generator (SG) leaks (i.e. smaller than a single tube guillotine failure size) places a reliance on the operators to manually undertake a controlled cool-down and reactor trip within a 50 minute period.

150 EDF and AREVA have provided a detailed substantiation report (Ref. 37) for both the deterministic and probabilistic claims for operator responses to SGTR faults. This has followed the Type C methodology. A summary of my assessment of this submission is provided in Appendix 4.

151 The substantiation has identified that the manual cool-down and reactor trip appears feasible for the scenarios considered within FS-04 within the required timescale. However there are several issues that need to be addressed to ensure that the task is achieved reliably within the 50 minutes claimed. These are detailed in HFIR items 50-54 and cover:

- Consideration of task sequencing to ensure a manual reactor trip (RT) can be achieved earlier.
- Addressing various identified HMI details including ensuring that there are sufficient HMI screens for the operator to use (the OA had problems being limited to 5 screens for showing desired PICS displays).
- Changing the power level for manual RT from 10% to 25% to ensure RT is undertaken earlier.
- Ensuring a clear and compelling cue when the power level drops to the required level for manual RT.

152 From my assessment of the HF submission (Ref. 37) I judge that a manual cool-down leading to a manual reactor trip can be reliably achieved providing the issues identified by the HFIR items 50-54 are adequately addressed by a future licensee. Consequently I consider that EDF and AREVA have provided sufficient justification for the reliance on manual actions for the deterministic SGTR case as required by Action **GI-UKEPR-FS-04.A2** on the basis that a future licensee will need to address the relevant HFIR issues (50-54). This is addressed by the general AF on HFIR items in section 4.7.

4.4.5 Start-up of Spent Fuel Pond Cooling Trains

153 As part of the Close-out for **GI-UKEPR-FS-03** on the Spent Fuel Pond (SFP) system EDF and AREVA have made claims for manual actuation of the SFP cooling system main trains as a first line of defence following failure of the normally operating system (Ref. 25). I have considered the HF aspects of these claims and note the following key points:

- The manual actions claimed appear to be readily feasible and are likely to be reliable given nature of the tasks and the long timescales required to undertake the necessary actions (a minimum of 2.4 hours in a worst case scenario but normally considerably longer).
- The HRA values currently used in the PSA model (10^{-4} for the MCR actions and $5x10^{-2}$ for the local to plant actions) may be optimistic; they will need to be re-evaluated in future revisions of the PSA.
- No appropriate substantiation has been provided for the claims for manual actions that support the preferred option for the design basis case.

154 I consider that the acceptability of reliance on manual actions as the ALARP option is dependent on the potential disadvantages arising from automation of the manual actions. This judgement is considered further in the Close-out report for GDA Issue **GI-UKEPR-FS-03**.

155 If the claims for manual action remain as part of the design basis case then an appropriate substantiation of the detailed HBSCs will need to be undertaken by a future licensee, along with a re-appraisal of the HRA values. I regard this as being a normal part of the HF safety case development post-GDA.

4.5 Assessment of Holistic Arguments & Evidence

156 EDF and AREVA have provided holistic arguments and evidence for the following topics:

- The approaches to minimise and mitigate the potential for misdiagnosis during fault conditions.
- How the operators will deal with fault situations with failed, or degraded, Automatic Diagnosis feature (AD).
- PICS to SICS / NCSS transfer.

4.5.1 The approaches to minimise and mitigate misdiagnosis during emergency operations

157 Misdiagnosis during emergency operations is recognised as being an important issue for nuclear power plants, particularly in the light of major incidents (e.g. Three Mile Island,) that needs to be addressed by both design and operational defences. At GDA Step 4 I judged that EDF and AREVA had not presented a sufficient case for how the UK EPR™ addressed misdiagnosis at the design stage.

158 EDF and AREVA have presented their case in a claims/arguments/evidence format (Ref. 39). The overall claim made for the consideration of misdiagnosis by EDF and AREVA is that the risk from operator misdiagnosis is minimised for post-fault management as:

- Sufficient barriers against operator misdiagnosis are provided.
- Sufficient recovery mechanisms for operator misdiagnosis are provided.

159 This claim is supported by several arguments with further supporting sub-arguments (see Ref. 39) as follows:

- A1: The SOA reduces the likelihood of misdiagnosis and, should misdiagnosis occur, will improve and support error detection and recovery.
- A2: The AD reduces the likelihood of misdiagnosis and, should misdiagnosis occur, will improve and support error detection and recovery.
- A3: The OS, SE, and SS roles provide an error prevention, detection and recovery contribution.
- A4: Detailed design of operating HMIs and procedures will minimise the opportunity for misdiagnosis.

160 My assessment has been based on my GDA Step 4 appraisal of the UK EPR™ control room and the detailed features claimed in Ref. 39 as defences against misdiagnosis. It has benefited from the detailed observations of the use of the HMI, SOA and MOP procedures in fault scenario simulations at the CNEN EPR™ simulator. This has provided me with a good understanding of the potential merits of the claimed defences.

161 EDF and AREVA have presented each of the arguments and sub-arguments in turn and described how they consider they provide either a barrier against misdiagnosis or a potential recovery mechanism. I consider that the defences operate frequently in combination and are inter-related. Consequently in additional to considering each element, I have considered two main cases holistically:

- The potential for misdiagnosis with the AD operating correctly.
- The potential for misdiagnosis with AD failure and operation from the SICS panels.

162 I consider that EDF and AREVA have presented a good summary of the main elements that help to reduce the potential for misdiagnosis and its recovery. My views of the key elements are described in the following paragraphs.

SOA approach

163 This approach is novel in the UK but has been progressively developed within the EDF French reactor fleet over more than 30 years. My evaluation of the SOA approach is that is has several notable features relevant to defence against misdiagnosis:

- It reduces the diagnosis burden on operators – no specific event diagnosis is required, instead a consideration of plant state based on a limited number of key safety functions.
- There are only 8 discrete SOA strategies to cover all main fault scenarios; entry/exit between them is dependent on consideration of the plant state and how each of the safety functions is being maintained or challenged.
- It requires continual ‘looping’ through a given SOA to ensure that the strategy remains applicable and that the plant state has not changed to a point requiring an alternative SOA strategy to be invoked.
- The looping approach provides a potential recovery from any cause of change of plant state – either plant failures or human error including earlier misdiagnosis.

164 The potential benefits of the SOA approach however are dependent on the technical accuracy of the procedures; the hierarchy of the SOA strategies and sub-strategies; and on the detailed navigation within, and between SOAs. These potential benefits are also dependent on the operating team roles (see below).

165 From my assessment of the post-fault claims substantiations, and observations in the EPR™ simulator I consider the SOA approach to be a defence for both reducing initial

misdiagnoses and as a recovery mechanism. However it does not eliminate the need for diagnosis though the nature of the diagnoses required is different. It is generally at a tactical level in determining the most appropriate means of achieving a particular safety function. I have noted this in several post-fault task analyses and EDF and AREVA have identified several HFIR issues on the need for specific information to be included within the procedures to ensure the operators are directed or alerted to the need to undertake particular actions; or to undertake specific systematic checks (e.g. for leak location identification). This further illustrates that that the detailed implementation of the SOA approach is an important factor as to how well the SOA approach provides defence against misdiagnosis.

166 The SOA approach and the determination of a limited number of its strategies based on plant state is novel to the UK. The technical basis for it, and its detailed strategies, have not been subject to detailed assessment during GDA Step 4. The technical basis for the UK EPR™ SOA strategies will need to be assessed in the future.

Automatic Diagnosis Feature

167 The AD feature on the UK EPR™ is new and stems from EDF's experiences with its N4 plants. The AD undertakes a systematic plant status check of key plant parameters to determine if SOA operation is required, and which SOA strategy criteria have been met. It has a visible and auditory alert and the AD display indicates the required SOA strategy that needs to be implemented. The AD provides continuous monitoring of plant state and re-alarms if there is a change in required SOA strategy.

168 I judge that this is a powerful support to successful SOA implementation and significantly reduces the operators' diagnostic task for SOA implementation. I consider that it will also provide a robust means of eventual recovery from any misdiagnosis that leads to plant states degrading to a point where an alternative SOA strategy is required.

169 Overall I consider that the AD feature when operating is a very effective barrier to misdiagnosis. However, when it is degraded or failed it presents a challenge as the operators may become overly dependent on it for evaluating SOA strategy and plant conditions. EDF and AREVA have made arguments on operation when it has failed – requiring operator evaluation using a plant status check that replicates the automatic AD processing either using the AD breakdown screens or via SICS panel parameter checks.

HMI Details

170 Argument A4 relates to the detailed HMI both minimising the potential for latent errors and by providing clear tactical level information to the operators. I consider the arguments to be appropriate and valid for any well designed modern HMI. There are some features for the UK EPR™ that I consider to be important:

- The provision of dedicated PICS status displays for implementation of each SOA phase used by both OA and OS. I believe this should assist them both co-ordinating their actions and in maintaining overall situational awareness.
- The provision of large computerised POP displays in addition to the 5 PICS monitors at each PICS workstation. These panels are potentially very useful in maintaining overall situational awareness and facilitating communications. In my GDA Step 4 assessment I raised an AF on the use of POP displays to support situational awareness. This submission on misdiagnosis further reinforces that AF as part of the defences against misdiagnoses.
- The PICS life sign indication – alerting the operators to degradation and failure of the PICS system.

- The separate and diverse PICS and SICS HMIs – providing a diverse means of Critical Safety Function (CSF) monitoring and control during SOA operation, including in event of PICS failure.
- The use of hyperlinks to route the operators to the correct control and procedures – this will minimise mis-selection errors and remove the need for the operators to diagnose that an inappropriate set of actions is being implemented.

171 On the prevention of latent errors, I note that EDF and AREVA have identified that detailed design and procedure development needs to be followed by robust verification and validation of both the HMI and procedures. This will need to be addressed post-GDA by a future licensee.

172 From my assessment I judge that the detailed PICS HMI including the AD feature should support reliable implementation of the SOA approach. However I note that some of the most useful PICS HMI features (AD, dedicated overview display, POPs) are not included in the SICS HMI, primarily due to the different technology employed for diversity reasons aided by the much greater simplicity of the functions covered by the SICS.

Procedures

173 Several of the sub-arguments presented are based on aspects of the procedures in providing defence against misdiagnosis notably:

- They will cover all SOA strategies and provide direction when AD failure occurs or other conditions requiring transfer away from the PICS workstations.
- The cycling through SOAs provides defence against any potential misdiagnosis.
- The procedures will provide all necessary tactical level information.

174 I accept the arguments made by EDF and AREVA on the role of procedures as a means of misdiagnosis defence. These would be similar for any modern nuclear power plant as well designed procedures should help to reduce both any initial misdiagnoses and provide potential recovery mechanisms.

175 For the UK EPR™ and the implementation of the SOA approach I have noted several positive features on the draft FA3 SOA procedures used during my simulator visit. I commented on these in my GDA Step 4 report; they include:

- Colour coding – both between and within the main OA and OS SOA procedures that assist in place keeping and co-ordination between OA and OS tasks.
- Separate OA and OS versions of the SOA strategy; the OS versions being tailored for strategy oversight and the OA version for detailed SOA method implementation.
- The use of computer presented MOPs for use by the OA in detailed implementation of specific control and monitoring tasks.
- The use of discrete phases within each SOA that assists in co-ordination between OA and OS (backed by colour coding).

176 I judge that these features are likely to provide some level of error prevention and recovery; including for misdiagnoses. The benefits of these features, and their potential use, should be considered in the development of the UK EPR™ procedures.

177 Overall I judge that the detailed SOA and MOP procedures that implement the SOA strategies potentially form a key defence against misdiagnosis. As acknowledged by EDF and AREVA, the quality of this defence will be dependent on the quality of the final

procedures. In particular I consider the following to be very important to maximise the potential misdiagnosis defence from the detailed procedures:

- Technical accuracy – including appropriate prioritisation; sequencing of SOA implementation; and entry/exit criteria between SOA strategies.
- Completeness and appropriate separation of guidance and instruction between the SOAs and associated MOPs.
- Inclusion of necessary specific guidance or instruction to ensure operators are alerted to the need for particular actions or to undertake systematic checking for important claimed operator actions (as identified by several HFIR items).
- Robust verification & validation of the detailed UK EPR™ SOA and MOP procedures – the SOA approach and AD feature are likely to lead to greater reliance on the procedures by the operators particularly if unusual conditions are met (e.g. AD failure; transfer to SICS panel operation).
- The usability of the procedures used to support manual SOA evaluation – either from the PICS AD breakdown displays or the SICS (and NCSS) panel instrumentation.

178 All the above will need to be addressed by a future licensee post-GDA within its design and safety case development work.

OS, SS and SE roles

179 EDF and AREVA consider that the OS potentially provides a barrier against misdiagnosis error by the OA; and that the SS and SE provide potential error recovery mechanisms due to their separate monitoring of the situation. I accept the basic arguments presented i.e. that each role can provide some level of defence against misdiagnosis.

180 However my judgment is that robust misdiagnosis defence stems from three basic roles that are formalised and embedded to a degree in the different procedures and HMIs used to perform these roles. These roles are:

- The OA undertaking detailed implementation of the SOA including control actions using the MOPs.
- The OS maintaining oversight of the SOA strategy and considering the need for significant navigation between SOA phases and between the SOA strategies – the OS is likely to provide some degree of misdiagnosis defence against OA errors:
  - By consultation and communication prior to OA actions – acting as an error barrier.
  - By monitoring of the overall strategy and hence detecting the outcomes of any OA misdiagnoses that lead to incorrect SOA implementation or the need to alter SOA strategy due to resulting plant state changes arising from any misdiagnosis.
- The SE monitoring of key safety functions from the SICS panel using dedicated SE procedures – this provides an element of diversity both in terms of the procedures and HMI used. This role is performed by the SS prior to the arrival of the SE (up to 40 minutes post-fault). This role is likely to be an effective, eventual recovery mechanism for any misdiagnosis or other error made by the OA and OS. However recovery by this route may only occur sometime after the initial misdiagnosis is made and possibly after a significant degradation in plant state has occurred.

181 The degree of defence provided by these roles will inevitably be dependent to some extent on the actual dynamics between the individuals performing each role. However a disciplined approach to the conduct of operations reinforced by suitable training should help to maximise the potential benefits from these role allocations. This will need to be considered by a future licensee post-GDA.

182 Although the SS does perform an additional role to the OA, OS and SE I do not consider that the role adds considerably to the error defence provided by the OS and SE roles. Indeed the supervisor will perform the SE role until the arrival of the SE which may be some time after the initial fault occurs.

Misdiagnosis Potential – AD operating correctly

183 Overall I consider that the combination of UK EPR™ HMI design features along with the SOA approach and operating concept (OA, OS and SE roles) provide robust defence against misdiagnosis. The HMI includes features that alert the operators if the AD is not working correctly, and the detailed displays allow the operators to check on state of parameters inputting to the AD assessment. The stated intent is that the operators will undertake a manual SOA state orientation is addition to AD evaluation.

184 In order to maximise the defence potentially offered by this combination there will need to be careful development of the detailed PICS HMI and procedures (SOA paper procedures and computerised MOPs) followed by robust verification and validation of both the HMI and procedures. This will need to be implemented by a future licensee post-GDA.

Misdiagnosis Potential – AD failure & non-PICS Situations

185 I consider that there is potentially a marked shift in reliance on operator diagnosis in situations without the AD feature operating. This places greater reliance on operator evaluation of the plant state and selection of the appropriate SOA and so considerably increases the potential for significant misdiagnosis.

186 EDF and AREVA have provided arguments for manual evaluation using either the AD breakdown displays or SICS panel instrumentation. Both manual evaluations are reliant on supporting paper based procedures. I consider that this is likely to require more time and be less reliable than the automatic AD process. Both the execution time and reliability are likely to be very dependent on the operators' knowledge and familiarity with manual evaluations using each HMI.

187 For SICS panel operation I consider that maintaining situational awareness is different to the approaches used for the PICS and POP HMIs. The operators will have to aggregate information from the SICS displays and continually check plant state without the support of various PICS features (e.g. the AD). Although the SICS HMI is similar to many conventional control room displays, the operators are unlikely to have the same familiarity with its detailed use (usage will primarily stem from training exercises) compared with operation from the PICS. A future licensee will need to consider the training needs, and what additional measures (e.g. paper based monitoring and decision support tools) could be provided to assist the operators in maintaining situational awareness as a key misdiagnosis defence.

188 Overall I consider that EDF and AREVA have made a sufficient case for addressing misdiagnosis for situations with AD failure or operation from the SICS panel at the GDA stage of design and procedure development. A future licensee will need to undertake further detailed work on:

- The detailed SICS panel HMI design – particularly on supporting situational awareness.

- Procedure development – especially for manual evaluation of plant state and SOA determination; and maintaining situational awareness.
- Training of operators to ensure adequate familiarity without support from the AD and for SICS panel operation.

Overall Conclusions for Misdiagnosis Potential

189 I consider that EDF and AREVA have presented a robust set of claims and supporting arguments to minimise the potential for misdiagnosis.

190 It has provided limited evidence to back the arguments made – but I judge that this is sufficient at this point in the design development process for GDA. Further evidence will need to be provided in the future once the detailed HMI and procedures have been developed.

191 I consider that the position when PICS and the AD system are operable is robust – the SOA approach and AD feature are significant barriers to misdiagnosis and provide effective recovery mechanisms.

192 I judge that the operating concept with OA, OS and SE roles assist in both limiting the potential for misdiagnosis, and provide potential recovery mechanisms.

193 I judge that the effectiveness of the claims and arguments presented are dependent to a considerable degree on:

- Future detailed HMI design and procedure development.
- Operator training and familiarity – especially for situations with AD failure and operation from the SICS panel.
- The detailed conduct of operations – to both maximise the roles of OS and SE in preventing and recovering from misdiagnosis.

194 I consider that all these issues form part of the normal design development process by a future licensee and normal business for ONR's continuing assessment. Additionally the AFs I have raised on the operating philosophy (**AF-UKEPR-HF-055**) and on the HFIR and HFAR items (see section 4.7) will ensure that a future licensee adequately addresses the above noted items.

4.5.2 Transfer from PICS to SICS interface

195 The deterministic safety case for the EPR™ indicates that the SICS panels are available as a back-up to the PICS primary workstations for key safety functions in event of PICS failure or unavailability. Additionally the PSA has encompassed claims for operator actions using the SICS workstation for scenarios with failure of the PICS.

196 The four PICS workstations use the PICS system for display and control of all plant parameters and use five monitors at each workstation. The PICS HMI is an advanced but very complex computerised system using computer presented procedures, mouse selection of icons for equipment controls; and incorporates the AD feature. The much simpler SICS panel uses conventional analogue displays, recorders and control devices (switches, buttons etc.). The SICS panels spread over a considerable length (3-4 metres) with three different panel areas. Each panel has three vertical levels of information with the top part used for alarm displays; the middle used for parameter information display; the lower level used for controls and instrumentation for operator control and feedback. These were considered in my GDA Step 4 assessment (Ref. 7).

197 On PICS system failure, severe degradation or unavailability the operators will have to transfer operations from the PICS workstations to the SICS panels and re-establish plant control. At GDA Step 4 I judged that this transfer of operations required further consideration due to the shift in HMI technologies and the potential challenges this might raise.

198 Although the physical transfer to SICS panel operation is straightforward and only requires actuation of two switches on the SICS panel (to enable SICS panel control and to disable PICS), there are challenges for effective transfer stemming from:

- A shift from an advanced computerised HMI with many support features (e.g. the AD, hyperlinks, detailed breakdown displays) to a conventional panel.
- A loss of the AD feature – and hence reliance on manual plant state and SOA evaluation without the support of the AD breakdown screens.
- A change in the procedures being used – with the SICS based procedures likely to require reference to additional paper based procedures to undertake discrete tasks (delaying actions that would be supported by computer presented MOPs).
- OA and OS unfamiliarity with operation from the SICS panel.
- How well the OA, OS allocation of roles works on the SICS panel.

199 EDF and AREVA have provided holistic claims, arguments and evidence (Ref. 40) to support the specific PSA claims for the transfer to, and operation from the SICS panel. Two claims are made along with several supporting arguments. The claims are:

1. The transfer from PICS to SICS supports reliable operation;
2. The SICS supports reliable operation.

200 My assessment has been built on my GDA Step 4 appraisal of the UK EPR™ control room and the detailed features claimed in this submission. My GDA Step 4 assessment benefited from the detailed observations of the use of the PICS HMI, SOA and MOP procedures in fault scenario simulations at the CNEN EPR™ simulator and on inspection of indicative SICS panels.

201 My assessment has focused on two areas:

- The validity of the claims and arguments presented – and the extent that the cited evidence confirms them.
- How well the case addresses potential key challenges for the transfer:
  - The reliance on manual plant state and SOA strategy evaluation
  - Re-establishing situational awareness and control from the SICS panel during evolving fault scenarios
  - How well the OA, OS and SE allocation of roles operates on the SICS panel
  - The lack of familiarity of the OA and OS in operating from a conventional panel, using different paper based procedures, for operator action claims in the immediate timescales following a transfer

202 I consider that EDF and AREVA have established a clear and appropriate strategy for ensuring an effective transfer from PICS workstation operation to SICS panel operations. The situations requiring transfer and associated transfer criteria have been determined, and the basis for supporting procedures has been established.

203 The arguments for PICS failure being clearly detectable appear reasonable; however I judge that insufficient evidence has been provided on the impact on operator responses to credible PICS failure modes and their means of degradation. My concern relates to partial PICS failure and any credible gradual degradation of PICS. Further confirmation for all credible PICS failure modes will need to be provided in the future.

204 I accept the arguments that reliable operation from the SICS panel is achievable with an appropriately designed SICS. EDF and AREVA have provided sufficient evidence of their approaches to ensure an adequate SICS panel and supporting procedures are developed. In essence the SICS panel represents other similar essential safety panels on nuclear power plants. The key requirements for the SICS panel are ensuring that it contains all control and instrumentation necessary for all its anticipated uses; and it is ergonomically well designed to match its intended operating use. The detailed design and procedures will need to be verified in the future. Inevitably personnel training on the transfer to, and operation from the SICS panel will be important to ensure reliable, effective operation.

205 At this point I do not consider that the arguments on the operating teams roles for operation from the SICS panel are fully supported. Further confirmation that maintaining the OA, OS roles when operating from the SICS panel is appropriate should be undertaken. The role of the SE appears to offer several useful benefits, but the practicability and most effective use of resource when all three personnel are operating from the same HMI should be considered further as part of the detailed development of the SICS design and associated procedures.

206 EDF and AREVA have not fully addressed the main challenges that I list above; in large part this appears to be due to lack of details of both the SICS panels and of the supporting procedures for transfer to, and operation from the SICS panel at this stage of the project. However I judge that EDF and AREVA have presented a reasonable case for SICS panel design and procedure development to underpin the SICS design at this point. A future licensee will have to undertake further work to ensure effective operational arrangements are developed for effective transfer to, and operation from the SICS panel.

207 From my assessment I judge that the main areas of uncertainty for the PICS to SICS transfer and SICS operation are:

- How quickly reliable transfer to, and re-establishment of situational awareness and control from the SICS panel can be achieved.
- The detailed transfer and operation procedures – especially manual SOA strategy evaluation – these are likely to have a considerable impact on how quickly and reliably SICS panel operations are achieved.
- The SICS panel HMI detailed design.

208 These uncertainties will need to be addressed by a future licensee. They are particularly important for the substantiation of any claimed operator actions from the SICS (or NCSS) panel in short timescales (e.g. under 30 minutes).

Overall conclusions for PICS to SICS transfer

209 I consider that EDF and AREA have presented a reasonable set of claims and supporting arguments to support reliable transfer from the PICS workstations to the SICS panels, and for reliable operation from the SICS panels.

210 I find that the arguments are generally adequately supported, but due to the lack of SICS panel design details and details of the key procedures it is not possible to fully confirm all the claims and arguments that are presented.

211 Further confirmation of the effectiveness of the PICS to SICS transfer, and reliable operation from the SICS panel will need to be undertaken by a future licensee. This is particularly important to support the substantiation of any claimed SICS (or NCSS) actions undertaken in short timescales from the transfer. In consequence I have raised an AF on PICS-SICS transfer and operation.

> ***AF-UKEPR-HF-59:*** *The Licensee shall provide further substantiation for PICS to SICS transfer and the time required to start reliable SICS (or NCSS) panel operation. It shall also justify that operating roles from the SICS panel can provide the most effective approach for operation from the SICS panel.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*

4.6 Assessment of Violation potential & minimisation

212 I considered violation potential as part of my work stream 1 GDA Step 4 assessment (Ref. 7). I concluded that although EDF and AREVA had presented arguments relating to approaches to minimise violation potential to ALARP insufficient evidence had been provided. Consequently I included the requirement to provide additional evidence to support the arguments as part of the GDA Issue.

213 Violations may stem from either design issues (e.g. difficult of access, difficulty of undertaking an action), or from operational causes (e.g. time pressure, conflicting goals). For GDA my focus is on the consideration of design related violations. This can be either aspects of the design that are likely to induce violations (e.g. making a task difficult); or for effective barriers to potential violations that can be identified and included in the design (e.g. interlock; ease of access).

214 EDF and AREVA have incorporated the consideration of violations into all of the Type A, B and C HFE substantiation methodologies (see Annex 1) employed during the Close-out of the GDA Issue GI-UK-EPR-HF-01 and resulting assessments. I have assessed the adequacy of consideration of design related violation potential as part of my methodology assessments.

215 The approaches EDF and AREVA have used are:

- Explicit consideration by use of a checklist with prompts words during workshops or HAZOPs using SMEs.
- Use of operational experience and information to identify issues and measures to address violations.
- Normal error reduction measures that are likely to both address errors and reduce the likelihood of violations (e.g. ensuring ease of access).

216 I consider that the approaches used are appropriate to identifying and addressing design related violations. I judge that their effectiveness during the assessments undertaken has been limited due to the lack of detailed design information at this point in the design. The assessments have identified some measures to be considered for identified violations; these are operational practice defences rather than design measures. These have generally been included in the HFIR items for further consideration and/or implementation by a future licensee.

217 EDF and AREVA's analysis of post-fault (Type C) HBSCs during GDA Close-out has not identified any credible violations arising during post-fault operations other than the operators potentially side-stepping procedural instructions to undertake a key action

earlier in a response. This type of violation is always possible however the operating concept (SOA applied by the OA, OS and SE) does provide an adequate level of defence.

218 Although EDF and AREVA have provided additional evidence on studies of existing EDF fleet operations (mainly for GDA Step 4) I consider that more could have been undertaken usefully earlier in the project to systematically identify known types of operational violations and to address these within the generic design. The additional measures EDF and AREVA have taken in response to the GDA Issue have provided additional evidence and confidence that violations have been given sufficient attention at this point in the design development. In conjunction with the material I assessed at GDA Step 4 I judge that EDF and AREVA have done sufficient to address violations for GDA However as the detailed design develops a future licensee will need to consider violation potential and defences further especially in determining the detailed HF requirements for systems and equipment procurement. This has been identified within HFIR items and consequently is encompassed by the AF I have raised on them in the following section.

4.7 Human Factors Issues and Assumptions Registers

219 Following on from queries I raised during the Close-out programme of work (particularly TQ-EPR-1600 see Annex 1) EDF and AREVA have developed a HFIR to record all significant issues arising from their analyses that require further consideration in order to ensure that the HBSCs are valid. The HFIR includes issues stemming from the GDA Step 4 submissions and those for closure of the HF GDA Issue **GI-UKEPR-HF-01**. EDF and AREVA have also developed a corresponding HFAR to record all the key assumptions used in the analysis.

220 As part of my assessment I have placed considerable attention on ensuring that the HFIR and HFAR adequately identify and record the issues and assumptions from each HBSC substantiation. From my detailed assessments I judge that the HFIR and HFAR have recorded important issues and assumptions that a future licensee needs to consider or implement them during future design and safety case development work post-GDA. In total 194 HFIR entries have been made; the vast majority of these stem from the Close-out submissions.

221 The HFIR entries provide specific details on issues that require consideration and resolution. Some identify specific recommendations for design modifications (e.g. automation of valves to remove the need for LTP actions; incorporation of specific information within the PICS HMI). From my assessment of the detailed submissions I consider that all the HFIR entries are appropriate and need to be addressed.

222 The assumptions register has recorded all the key assumptions used in the HF Close-out work. The assumptions include aspects relating to:

- Roles and duties of the OA, OS and SE.
- Operational & maintenance practices, including administrative controls.
- Content and format of procedures.
- Future details of the UK EPR™ HMIs, including NCSS design and operation.
- Refinements in transient analyses and safety cases showing less demanding. requirements for certain HBSCs.

223 I consider that the assumptions are appropriate and form an important part of the substantiations. A future licensee will need to ensure that they remain valid or if changes

that affect these assumptions are made then the relevant claim is revised in the light of the actual design at that point.

224 EDF and AREVA updated and consolidated its HF Tracking Registers at the end of the GDA Close-out work to Revision 1. This has consolidated the HF Issues and Assumptions and renumbered the HF Issues. A future licensee will need to consider the detailed HFIR items and assumptions identified in each specific submission as part of its future work. Annexes 4 and 5 detail the HFIR items identified from the assessed submissions.

225 I conclude that the HFIR and HFAR together provide a concise summary of key issues stemming from the HF safety case that a future licensee needs to address in its future development of the detailed design and operating practices for a UK EPR.

> ***AF-UKEPR-HF-60:*** *The Licensee shall address and implement all the items identified from the GDA HF assessments in the HF Issues and Assumptions Registers, or provide a justification for any alternative position taken on any given item. It should also provide ONR with a programme showing where and when in its future work it envisages addressing each HFIR item and HFAR assumptions.*
>
> ***Required timescale:*** *Prior to First structural concrete*

4.8 Provision of a UK HF Safety Case

226 Action A2 of the GDA Issue required EDF and AREVA to provide a HF safety case that was consistent with the expectations of ONR and suitable for the UK context. It also required the relevant presentation of the HF safety case in the PCSR to be updated to reflect this case.

227 I judge that the very considerable work undertaken by EDF and AREVA to address action A1 of the GDA Issue in conjunction with the basis that I assessed in my Step 4 report now represents a comprehensive HF safety case for this stage in the design. Although there are aspects that are based on assumptions I judge from my assessments that these assumptions are reasonable and as expected at this stage of the design development.

228 EDF and AREVA have identified and provided substantiation for all the risk significant HBSCs in a claims/arguments/evidence format. This has been complemented by claims/arguments/evidence for the underpinning approaches taken by EDF and AREVA to take account of the potential for human interaction with the plant during operation and maintenance, including all post-fault response requirements.

229 EDF and AREVA have provided an updated PCSR that now reflects this updated safety case. Chapter 18.1 of the PCSR presents the main case with support from Chapter 18.3 (November 2012). Additionally other parts of the PCSR have been amended to reflect the changes stemming from this updated HF safety case.

230 I have assessed the revised PCSR. I consider that it now provides a presentation of the overall HF safety case for the UK EPR™ in a manner that supports the basis claims, arguments and evidence expectations for the UK. This includes presentation of the elements of the case that I assessed at Step 4 combined with those additional studies undertaken to Close-out action A1 of the GDA Issue **GI-UKEPR-HF-01**.

231 My assessment of Chapter 18.1 (and 18.3) of the revised PCSR (November 2012) leads me to conclude that:

- This now presents an accurate high level summary of the overall HF safety case (both the elements I assessed at Step 4 and the new studies in response to the GDA Issue **GI-UKEPR-HF-01**).
- It is presented in a claims, arguments, evidence format that well matches ONR's expectations for the UK.
- It, and the HF safety case it summarises, meets the requirements of the GDA Issue action.

232 I consider that the presentation of the HF safety case now provides a useful template for a large project of this nature at the PCSR stages.

5 ASSESSMENT FINDINGS

233 As noted in section 1.1 AFs are findings that are identified during the regulators' GDA assessment that are important to safety, but not considered critical to the decision to start nuclear island safety related construction of such a reactor. I raised 54 AFs during GDA Step 4 that should be implemented through a forward programme for the UK EPR™ as routine regulatory business.

234 During my assessment of the submissions provided by EDF and AREVA to close-out GDA Issue **GI-UKEPR-HF-01** I have raised a further 6 AFs. These should be addressed by a future licensee alongside those raised during GDA Step 4. The numbering of the AFs raised during the GDA Issue Close-out stage follows on from those raised during GDA Step 4.

235 It should be noted that AF ***AF-UKEPR-HF-60*** is very extensive as it includes all the discrete HFIR items and significant assumptions capture in the HFIR and HFAR registers. Many of the HFIR items are likely to lead to design and /or changes to the UK EPR safety case at a detailed, but potentially important level. Collectively it reinforces the value of the HF GDA Issue and close-out work as part of the overall GDA process

5.1 Additional Assessment Findings

236 The additional AFs raised during Close-out of GDA Issue **GI-UKEPR-HF-01** are:

> ***AF-UKEPR-HF-55:*** *The Licensee shall ensure that its operating philosophy is consistent with the assumptions made in the GDA HF substantiations on the use of the SOA approach, procedures, and on the key operating roles of Action and Strategy Operators (OA and OS) and the Safety Engineer (SE). If an alternative approach is intended by the licensee then re-justification of all relevant HBSCs will be required and re-analysis as necessary.*
>
> **Required timescale:** Prior to First structural concrete.
>
> ***AF-UKEPR-HF-56:*** *The Licensee shall determine the impact of credible degradation and failure modes of the C&I systems on the PICS displays and their resulting impact on any claimed operator actions. The licensee will need to re-substantiate any affected HBSCs.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*
>
> ***AF-UKEPR-HF-57:*** *The Licensee shall determine the most effective use and presentation of alarms to support claimed operator actions during SOA and OSSA operations. This shall include consideration of the use of the Plant Overview Panels as a means of displaying alarms and how any specific alarm monitoring should be included in SOA operation by both the OA, OS team and the SE.*
>
> ***Required timescale:*** *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*
>
> ***AF-UKEPR-HF-58:*** *The Licensee shall determine if internal floods generate alarms that are likely to mask or delay response to key alarms or indications prompting operators to undertake claimed leak response actions. The licensee shall provide an appropriate justification that any claimed operator actions required to support the Internal Hazards flooding case are reliably achievable within the required timescales.*

Required timescale: *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*

AF-UKEPR-HF-59: *The Licensee shall provide further substantiation for PICS to SICS transfer and the time required to start reliable SICS (or NCSS) panel operation. It shall also justify that operating roles from the SICS panel can provide the most effective approach for operation from the SICS panel.*

Required timescale: *Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning*

AF-UKEPR-HF-60: *The Licensee shall address and implement all the items identified from the GDA HF assessments in the HF Issues and Assumptions Registers, or provide a justification for any alternative position taken on any given item. It should also provide ONR with a programme showing where and when in its future work it envisages addressing each HFIR item and HFAR assumptions.*

Required timescale: *Prior to First structural concrete*

5.1.1 Impacted GDA Step 4 Assessment Findings

237 No AFs raised during GDA Step 4 were impacted by the Close-out of GDA Issue **GI-UKEPR-HF-01**. Therefore all AFs raised during GDA Step 4 remain valid and should be addressed by a future licensee wishing to construct a UK EPR™.

6 ASSESSMENT CONCLUSIONS

238 The overall conclusions from my assessment for the Close-out of GDA Issue **GI-UKEPR-HF-01** are shown below.

6.1 Overall Conclusions for Action GI-UKEPR-HF-01.A1

239 EDF and AREVA have undertaken considerable work to address each part of GDA Issue Action A1 to complete identification and substantiation of HBSCs. This work has been of very good quality and generally at a detailed level. In total I judge that this represents a commendable response by EDF and AREVA to fully address the GDA Issue.

240 I consider that the identification of risk significant Type A pre-fault HFEs has been completed as far as is reasonably practicable at this point – the limitation being the lack of detailed information on the detailed design and procedures at this point in the design development process.

241 From my assessment I judge that the Type A & B pre-fault HFEs have been partially substantiated – the work has focussed on those Type A & B HFEs that are most likely to be significant to risk. I find that the substantiations provided are based on reasonable assumptions about the detailed design, maintenance and operations, including the supporting procedures. Key assumptions have been recorded in the HFAR.

242 Documentation on the substantiation of all risk significant (i.e. the high and medium risk) Type C post-fault HFEs has been provided. I consider that only a few of the Type C HFEs has fully substantiated; the majority of the HFEs have been partially substantiated. In cases where partial substantiation has been submitted I judge that the issues and assumptions requiring further consideration or implementation have been identified and are recorded in the HFIR and HFAR. This confirms the preliminary view that I made at GDA Step 4 that an acceptable position can be reached for all the Type C HFEs that have not been fully substantiated to date.

243 I consider that EDF and AREVA have provided satisfactory holistic arguments and evidence to support their claims on the role of SOA and AD in reducing the potential for misdiagnosis; and on how the situations with failed AD are addressed satisfactorily. EDF and AREVA have also provided additional holistic arguments and some evidence on the transfer from PICS to SICS (and NCSS) panel operation in the event of C&I failures. This has not identified any significant design issues, but will require further consideration post-GDA to verify the most appropriate operating arrangements from the SICS panel.

244 I consider that EDF and AREVA's consideration of the prevention and mitigation of design related violations has been limited. It has primarily been undertaken within their Type A and C analysis approaches. However I judge that further consideration of potential for violations and their appropriate defences can be made as the design and operational details are developed post-GDA.

245 EDF and AREVA have identified a significant number of detailed HF issues and key underpinning assumptions that need to be further considered or implemented by a future licensee; my own assessment has identified additional items. I have encompassed all these within a few detailed AFs that, in conjunction with the AFs identified at GDA Step 4, will need to be addressed by a future licensee.

246 I judge that the combination of work undertaken to address the GDA Issue **GI-UKEPR-HF-01** combined with the submissions I assessed at Step 4 have ensured that the UK EPR™ design is sufficient to meet ALARP requirements at this point in the design process. A future licensee will need to address all the AFs raised both in this report and

the Step 4 HF Assessment report to ensure ALARP requirements are met as the detailed design is developed.

6.2 Overall Conclusions for Action GI-UKEPR-HF-01.A2 – Review of the Update to the PCSR

247 I consider that the substantiation work provided by EDF and AREVA, in combination with the material submitted for the GDA Step 4 assessment, now comprise a comprehensive HF safety case for the UK EPR™ that generally matches ONR's expectations for GDA.

248 The revised Chapter 18 of the PCSR now provides an acceptable summary of this overall HF safety case. I consider that it provides a clear presentation of all the significant claims, arguments and supporting evidence for the HF safety case.

6.3 Overall Closure of GI-UKEPR-HF-01

249 Overall I consider that EDF and AREVA have addressed each part of the issue **GI-UKEPR-HF-01**, and provided the necessary substantiations and consolidated safety case. The concerns that need to be further addressed by a future licensee are ones that can be readily incorporated into the normal design and safety case development refinements expected post-GDA. My assessment has not identified anything that forecloses options associated with HF. On this basis I judge that this GDA Issue can be closed.

7 REFERENCES

1 *ONR HOW2 Business Management System. Assessment Process.* PI/FWD – Issue 3. HSE. April 2010. www.hse.gov.uk/nuclear/operational/assessment/index.htm.

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

3 *ND BMS. Technical Assessment Guides:*

- *ND Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable*). T/AST/005 Issue 4, Revision 1. HSE. January 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast005.htm
- *Early initiation of safety systems.* T/AST/010 Issue 2. HSE. July 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast010.htm
- *Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.* T/AST/051 Issue 1. HSE. May 2002. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast051.pdf
- *Human Factors Integration.* T/AST/058 Issue 1. HSE. September 2010. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast058.htm
- *Human Machine Interface.* T/AST/059 Issue 1. HSE. November 2010. www.hse.gov.uk/foi/internalops/tech_asst_guides/tast059.htm
- *Human Reliability Analysis.* T/AST/063 Issue 1. HSE. March 2010. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast063.htm

4 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels.* WENRA. January 2008. www.wenra.org.

5 *Safety of Nuclear Power Plants: Design. Safety Requirements.* International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-R-1. IAEA. Vienna. 2000. www.iaea.org.

6 *GDA Issue GI-UKEPR-HF-01 Revision 0. Identification and Substantiation of Human Based Safety Claims.* ONR. July 2011. TRIM Ref. 2011/385307.

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

8 *Resolution Plan for GDA Issue GI-UKEPR-HF-01 Revision 0.* EDF and AREVA. July 2011. TRIM Ref. 2011/289099.

9 *Reference Design Configuration*. UKEPR-I-002 Revision 15. EDF and AREVA. December 2012. TRIM Ref. 2012/478281.

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

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

12 *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.

13 *EDF and AREVA UK EPR™ - Schedule of Technical Queries Raised during GDA Step 1 to Step 4.* HSE-ND. TRIM Ref. 2010/600726.

14 *EDF and AREVA UK EPR™ - Schedule of Regulatory Observations Raised during GDA Step 1 to Step 4.* HSE-ND. TRIM Ref. 2010/600727.

15 *EDF and AREVA UK EPR™ - Schedule of Regulatory Issues Raised during GDA Step 1 to Step 4. HSE*-ND. TRIM Ref. 2010/600728.

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

17 *EDF/AREVA GDA Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors.* 17163-707-000-RPT-0001 Issue 4. AMEC. June 2011. TRIM Ref. 2011/359206.

18 *EDF/AREVA GDA Task Analysis: Example Pre-Fault Analysis*. 16474/TR/005 Issue 02. AMEC. November 2010. TRIM Ref. 2011/85811.

19 *Equipment Reliability Process Description.* AP913 Revision 1. Institute of Nuclear Power Operations (INPO). November 2001.

20 *Preventive Maintenance Basis - Overview Report* TR-106857 Revision 1. Electric Power Research Institute (EPRI). 1998.

21 *Preventative Maintenance Information Repository (PMIR): Functional Specification*. Reference 1000702. Electric Power Research Institute (EPRI). November 2000.

22 *EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims*. 16474/TR/0003 Issue 02. AMEC. September 2010. TRIM Ref. 2011/92916.

23 *EDF/AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK].* 16474-TR-006 Issue 01. AMEC. December 2010. TRIM Ref. 2011/85812.

24 *Guiding Principles Relating to the Organization of the Flamanville 3 Shift Crew.* D4002.92-07/084. EDF. February 2010. TRIM Ref. 2011/93918.

25 *Analysis of a Class 1 requirement for the PTR (FPPS/FPCS) start-up feature of the main cooling trains.* ECECS120406 Revision A. EDF. May 2012. TRIM ref. 2012/211370.

26 *GDA Issue GI-UKEPR-IH-01 Revision 2 - Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the EPR design*. ONR. July 2011. TRIM Ref. 2011/385308.

27 *GDA Issue GI-UKEPR-IH-03 Revision 2 - Internal Flooding Safety Case*. ONR. July 2011. TRIM Ref. 2011/385310.

28 *GDA Issue GI-UKEPR-FS-01 Revision 0 - Heterogeneous Boron Dilution Safety case.* ONR. July 2011. TRIM Ref. 2011/385301.

29 *GDA Issue GI-UKEPR-FS-04 Revision 1 - Steam Generator Tube Rupture Safety Case.* ONR. July 2011. TRIM Ref. 2011/385304.

30 *UK EPR™ Safety Case for Heterogeneous Boron Dilution Fault.* PEPC-F DC 70 Revision B. Areva. September 2012. TRIM Ref. 2012/381247.

31 *UK EPR™ Design Improvements for Heterogeneous Boron Dilution Faults.* PEPR-F DC 97 Revision A. Areva. June 2012. TRIM Ref. 2012/240887.

32 *EDF/AREVA GDA Human Factors Issue: Heterogeneous Boron Dilution.* 16895-707-000-RPT-014 Issue F-BPE. AMEC. August 2012. TRIM Ref. 2012/344349.

33 Not used

34 *UK EPR™ – Internal Flooding – Multi-legged safety case and ALARP consequence assessment analyses.* ECEIG121115 Revision B. EDF. September 2012. TRIM Ref. 2012/377087.

35 EDF/AREVA GDA Human Factors: Internal Flooding. 16895-707-000-RPT-0013 Issue E-BPE. AMEC. September 2012. TRIM ref. 2012/364866.

36 *Steam Generator Tube Rupture Mitigation Strategy.* PEPR-F DC 38 Revision D. Areva. October 2012. TRIM ref. 2012/386453.

37 *EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies Post fault task analysis of "SGTR 1 tube" and claims OP_SCD_30MN and OPE_SGTR.* 16895-707-000-RPT-0002 Issue I-BPE. AMEC. October 2012. TRIM Ref. 2012/417079.

38 *GDA Issue GI-UKEPR-FS-03 Revision 0 - Spent Fuel Pool Safety Case.* ONR. July 2011. TRIM Ref. 2011/385303.

39 *EDF/AREVA/ GDA Human Factors: Holistic Arguments and Evidence to Support Claims relating to Misdiagnosis in Emergency Operations.*16895-707-000-RPT-015 Issue F-BPE. AMEC. August 2012. TRIM Ref. 2012/338598.

40 *EDF/AREVA GDA Human Factors: PICS to SICS transfer: A claims, argument and evidence-based safety case*. 16895-707-000-RPT-017 Issue G-BPE. AMEC. August 2012. TRIM Ref. 2012/339458.

41 *UK EPR: EDF AREVA Task analysis method statement – Claim 2: Prefault Human Errors and Human Errors performed on systems and equipment not modelled in PSA.* (Annex to letter EPR00591N) ECEF102051. Revision A. EDF. TRIM Ref. 2011/134476.

42 *RO-UKEPR-38 - Update of the Methodology for the Analysis of Type A Human Based Safety Claims.* Letter from UK EPR Project Front Office to ONR. Unique Number EPR00847N. 18 April 2011. TRIM Ref. 2011/230231.

43 *EDF/AREVA GDA Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors arising from Maintenance, Testing and Calibration*. 17163-707-000-RPT-0001 Issue 6. AMEC. September 2011. TRIM Ref. 2011/512156.

44 *UK GDA Analysis of Pre-Initiator Human Errors – Risk Significant Equipment Grouped by Generic Equipment Type (Including Legacy - Non-Legacy Status).* 17163-190-000-RPT-0001 Issue 2. AMEC. August 2011. TRIM Ref. 2011/411901.

45 *Identification of Tasks Associated with Type A/B Human Failure Events Modelled in the PSA.* 17163-707-000-RPT-0002 Issue F-BPE. AMEC. February 2012. TRIM Ref. 2012/85127.

46 *Task Analysis (Human HAZOP) Programme for Type A/B Human Failure Events Modelled in the PSA.* 17163-707-000-RPT-0003 Issue D-BPE. AMEC. February 2012. TRIM Ref. 2012/85130.

47 *Task Analysis (Human HAZOP) Programme for Type A/B Human Failure Events Modelled in the PSA.* 17163-707-000-RPT-0003 Issue F-BPE. AMEC. May 2012. TRIM Ref. 2012/225067.

48 *Substantiation of Identified Type A Human Failure Events Modelled in the PSA.* 17163-707-000-RPT-0004 Issue H-BPE. AMEC. August 2012. TRIM Ref. 2012/342881.

49 *Confirmation of design features relating to misalignment of automated valves.* PEPSPF/11.486 Revision 1. Areva. December 2011. TRIM Ref. 2011/655684.

50 *EPR UK GDA Issue HF01 – report D1.7: Substantiation of identified type B human failures events.* ECSN120755 Revision A. EDF. October 2012. TRIM Ref. 2012/426167.

51 *Dropped loads and Fuel Handling: Methodology for the Identification of the Human Based Safety Claims.* PEPS-F DC 96 Revision B. Areva. October 2011. TRIM 2011/532547.

52 *Dropped loads and Fuel Handling: Methodology for the Identification of the Human Based Safety Claims.* PEPS-F DC 96 Revision D. Areva. January 2012. TRIM Ref. 2012/31318.

53 *Identification of Dropped Load and Fuel Handling Human Based Safety Claims – Polar Crane*. PEPS-F DC 134 Revision B. Areva. June 2012. TRIM Ref. 2012/259642.

54 *Identification of Dropped Loads and Fuel Handling Based Safety Claims – Refuelling Machine.* PEPS-F DC 135 Revision B. Areva. July 2012. TRIM Ref. 2012/265588.

55 *EDF/AREVA GDA Human Factors: Heterogeneous Dilution Methodology*. 16895-707-000-RPT-0014 Issue B-PREL. AMEC. December 2011. TRIM Ref. 2011/655701.

56 *EDF/AREVA Human Factors Issue: Heterogeneous Boron Dilution.* 16895-707-000-RPT-0014 Issue F-BPE. AMEC. August 2012. TRIM Ref. 2012/344349.

57 *UK EPR - Identification and Categorisation of PSA 2011 Type C claims*. PEPSPF/11.304. Areva. July 2011. TRIM Ref. 2011/403777.

58 *EDF/Areva – GI-UKEPR-HF-01 Deliverable D2.2 - Schedule of Intermediate Type C Task Analyses.* Letter from UK EPR Project Front Office to ONR. Unique Number EPR00908R. 15 July 2011. TRIM Ref. 2011/379015.

59 *EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies – Post fault task analysis of "SGTR1 tube" and claims OP_SCD 30MN and OPE_SGTR.* 16895-707-000-RPT-002 Issue F-BPE. AMEC. March 2012. TRIM Ref. 2012/121267.

60 *EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies – Post Fault Task Analysis of "SGTR 1-tube" and claims [OP_SCD_30MN] and OPE_SGTR*. 16895-707-000-RPT-002 Issue I-BPE. AMEC. October 2012. TRIM Ref. 2012/417079.

61 *EDF/AREVA GDA Human Factors: Internal Flooding*. 16895-707-000-RPT-0013. Issue C-BPE. AMEC. June 2012. TRIM Ref. 2012/259143.

62 *EDF/AREVA GDA Human Factors: Internal Flooding*. 16895-707-000-RPT-0013 Issue E-BPE. AMEC. September 2012. TRIM Ref. 2012/364866.

63 *EDF/AREVA GDA Task Analysis: Feed and Bleed Recovery Strategies [OP-BLEED_120MN} & [OP-BLEED-30MN].* 16895-707-000-RPT-0001 Issue D-PREL. AMEC. July 2011. TRIM Ref. 2011/403779.

64 *EDF/AREVA GDA Task Analysis of Post Fault Claim H2 [OP_LHSI_IND_120MN].* 16895-707-000-RPT-003 Issue E-BPE. AMEC. March 2012. TRIM Ref. 2012/102575.

65 *EDF/AREVA GDA Task Analysis of Post Fault Claim H2 [OP_LHSI_IND_120MN].* 16895-707-000-RPT-003 Issue H-BPE. AMEC. October 2012. TRIM Ref. 2012/408990.

66 *Task Analysis of Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M].* 16895 -707-000-RPT-0004 Issue D-BPE. AMEC. July 2012. TRIM Ref. 2012/230968.

67 *EDF/AREVA GDA: Task Analysis of Post Fault Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M].* 16895 -707-000-RPT-0004 Issue F-BPE. AMEC. October 2012. TRIM Ref. 2012/436940.

68 *EDF/AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK]*. 16474-TR-006 Issue G-BPE. AMEC. May 2012. TRIM Ref. 2012/206357.

69 *EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims*. 16474-TR-003 Issue D-BPE. AMEC. May 2012. TRIM Ref. 2012/224378.

70 *EDF/AREVA GDA Task Analysis of Post-Fault Claims M6 [OP_FSCD_30MN-IH], M8 [OPE_52] and M19 [OP_COMBI_240MN_LDEP]*. 16895-707-000-RPT-005 Issue D-BPE. AMEC. September 2012. TRIM Ref. 2012/391024.

71 *EDF/AREVA GDA Task Analysis: Entry into the Severe Accident Management Guidelines (OSSA).* 16895-707-000-RPT-0006 Issue E-BPE. AMEC. August 2012. TRIM Ref. 2012/343734.

72 *EDF/AREVA Task Analysis: Primary Circuit depressurisation in the EOP and OSSA*. 16895-707-000-RPT-0007 Issue D-BPE. AMEC. October 2012. TRIM Ref. 2012/389245.

73 *EDF/AREVA Task Analysis: Operator Responses to Loss of Instrumentation and Control [OP_EFWS]*. 16895-707-000-RPT-0008 Issue D-BPE. AMEC. September 2012. TRIM Ref. 2012/381449.

74 *EDF/AREVA GDA Task Analysis: Operator Response to decreasing RCS Level [OP_SIS_INJ_80MN_NCSS] on the Non Computerised Safety System*. 16895-707-000-RPT-0010 Issue E-BPE. AMEC. May 2012. TRIM Ref. 2012/206293.

75 *EDF/AREVA GDA Task Analysis: Operator Response to decreasing RCS Level [OP_SIS_INJ_80MN_NCSS] on the Non Computerised Safety System.* 16895-707-000-RPT-0010 Issue G-BPE. AMEC. October 2012. TRIM Ref. 2012/426247.

76 *EPR UK GDA – Human Factors – Time estimate for transfer to NCSS.* ECUK121139 Revision A. EDF. October 2012. TRIM Ref. 2012/426248.

77 *EDF/AREVA GDA Task Analysis: NCSS Action for OP_BLEED_30MN_NCSS.* 16895-707-0000-RPT-0024 Issue D-BPE. AMEC. August 2012. TRIM Ref. 2012/344415.

78 *EDF/AREVA GDA Task Analysis: NCSS Action for [OP_EFW_NCSS], [OP_FB_120M_MDEP_NCSS], [OPE_52_LOCAL], [OP_SBODG_LOCAL]*. 16895-707-0000-RPT-0011 Issue D-BPE. AMEC. October 2012. TRIM Ref. 2012/411718.

79 *GI-UKEPR-HF-01 – Confirmation of Design Features Related to Claims M3/M23/M25/M28*. PEPSF/12.104 Revision 1. Areva. March 2012. TRIM Ref. 2012/147813.

80 *EDF/AREVA GDA Task Analysis Summary Report*. 16895-707-000-RPT-025 Issue C-BPE. AMEC. November 2012. TRIM Ref. 2012/467520.

81 *EDF/AREVA GDA Human Factors: Holistic arguments and evidence to support claims relating to misdiagnosis in emergency operations*. 16895-707-000-RPT-0015 Issue F-BPE. AMEC. August 2012. TRIM Ref. 2012/338598.

82 *EDF/AREVA GDA Human Factors: PICS to SICS transfer: A claims, arguments and evidence-based safety case.* 16895-707-000-RPT-0017 Issue G-BPE. AMEC. August 2012. TRIM Ref. 2012/339458.

83 *EDF/AREVA GDA Human Factors: PCSR Sub-Chapter 18.1 Revised Structure*. 16895-707-000-RPT-0018 Issue B-PREL. AMEC. December 2011. TRIM Ref. 2012/386.

84 *PCSR Sub-Chapter 18.1 - Human Factors*. UKEPR-0002-181 Advance Version of Issue 06. EDF. 2012. TRIM Ref. 2012/343709.

85 *PCSR Sub-Chapter 18.1 - Human Factors.* UKEPR-0002-181 Issue 06. EDF. November 2012. TRIM Ref. 2012/450490.

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A1		ECEF102051, Rev. A	UK EPR: EDF AREVA Task analysis method statement for Prefault Human Errors and Human Errors performed on systems and equipment not modelled in PSA	41
GI-UKEPR-HF-01.A1		EPR00847N	Update of the Methodology for the Analysis of Type A Human Based Safety Claims	42
GI-UKEPR-HF-01.A1	D1.1	17163-707-000-RPT-0001, Issue 4	EDF/AREVA GDA Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors	17
GI-UKEPR-HF-01.A1	D1.1	17163-707-000-RPT-0001, Issue 6	EDF/AREVA GDA Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors arising from Maintenance, Testing and Calibration	43
GI-UKEPR-HF-01.A1	D1.2	17163-190-000-RPT-0001, Issue 2	UK GDA Analysis of Pre-Initiator Human Errors – Risk Significant Equipment Grouped by Generic Equipment Type (Including Legacy - Non-Legacy Status)	44
GI-UKEPR-HF-01.A1	D1.3	17163-707-000-RPT-0002 F-BPE	Identification of Tasks Associated with Type A/B Human Failure Events Modelled in the PSA	45
GI-UKEPR-HF-01.A1	D1.4	17163-707-000-RPT-0003 D-BPE	Task Analysis (Human HAZOP) Programme for Type A/B Human Failure Events Modelled in the PSA	46
GI-UKEPR-HF-01.A1	D1.4	17163-707-000-RPT-0003 F-BPE	Task Analysis (Human HAZOP) Programme for Type A/B Human Failure Events Modelled in the PSA	47

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A1	D1.5	17163-707-000-RPT-0004 H-BPE	Substantiation of Identified Type A Human Failure Events Modelled in the PSA	48
GI-UKEPR-HF-01.A1	D1.6	PEPSPF/11.486 Rev. 1	Confirmation of design features relating to misalignment of automated valves	49
GI-UKEPR-HF-01.A1	D1.7	ECESN120755 Rev. A	Substantiation of identified type B human failures events	50
GI-UKEPR-HF-01.A1	D1.8	PEPS-F DC 96, Rev. A	Dropped loads and Fuel Handling: Methodology for the Identification of the Human Based Safety Claims	51
GI-UKEPR-HF-01.A1	D1.9	PEPS-F DC 96, Rev. D	Dropped loads and Fuel Handling: Methodology for the Identification of the Human Based Safety Claims	52
GI-UKEPR-HF-01.A1	D1.10a	PEPS-F DC 134 Rev B	Identification of Dropped Load and Fuel Handling Human Based Safety Claims – Polar Crane	53
GI-UKEPR-HF-01.A1	D1.10b	PEPS-F DC 135 Rev B	Identification of Dropped Loads and Fuel Handling Based Safety Claims – Refuelling Machine	54
GI-UKEPR-HF-01.A1	D1.11	16895-707-000-RPT-0014 BPREL	EDF/AREVA GDA Human Factors: Heterogeneous Dilution Methodology	55
GI-UKEPR-HF-01.A1	D1.11	16895-707-000-RPT-0014 F-BPE	EDF/AREVA Human Factors Issue: Heterogeneous Boron Dilution, AMEC report	56
GI-UKEPR-HF-01.A1	D2.1	PEPSPF/11.304	Identification and Categorisation of PSA 2011 Type C claims	57
GI-UKEPR-HF-01.A1	D2.2	EPR00908R	Schedule of intermediate Type C task analyses	58

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A1	D2.3	16895-707-000-RPT-002, Issue F-BPE	EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies	59
GI-UKEPR-HF-01.A1	D2.3	16895-707-000-RPT-002, Issue I-BPE	EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies – Post Fault Task Analysis of "SGTR 1-tube" and claims [OP_SCD_30MN] and OPE_SGTR	60
GI-UKEPR-HF-01.A1	D2.4	16895-707-000-RPT-0013, Issue C-BPE	EDF/AREVA GDA Human Factors: Internal Flooding	61
GI-UKEPR-HF-01.A1	D2.4	16895-707-000-RPT-0013, Issue E-BPE	EDF/AREVA GDA Human Factors: Internal Flooding	62
GI-UKEPR-HF-01.A1	D2.5 R1 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0001, Issue 1	EDF/AREVA GDA Task Analysis: Feed and Bleed Recovery Strategies [OP-BLEED_120MN} & [OP-BLEED-30MN]	63
GI-UKEPR-HF-01.A1	D2.5 R3 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-003, Issue E-BPE	EDF/AREVA GDA Task Analysis of Post Fault Claim H2 [OP_LHSI_IND_120MN]	64
GI-UKEPR-HF-01.A1	D2.5 R3 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-003, Issue G-BPE	EDF/AREVA GDA Task Analysis of Post Fault Claim H2 [OP_LHSI_IND_120MN]	65
GI-UKEPR-HF-01.A1	D2.5 R4 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0004, Issue D-BPE	Task Analysis of Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M]	66
GI-UKEPR-HF-01.A1	D2.5 R4 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0004, Issue F-BPE	Task Analysis of Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M]	67

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A1	D2.5 (final version of example provided at GDA Step 4)	16474-TR-006 G-BPE	EDF/AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK]	68
GI-UKEPR-HF-01.A1	D2.5 (final version of example provided at GDA Step 4)	16474-TR-003 D-BPE	EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims	69
GI-UKEPR-HF-01.A1	D2.5 R5(not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-005, Issue D-BPE	EDF/AREVA GDA Task Analysis of Post-Fault claims M6 [OP_FSCD_30MN-IH], M8 [OPE_52] and M19 [OP_COMBI_240MN_LDEP]	70
GI-UKEPR-HF-01.A1	D2.5 R6 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0006-E-BPE	EDF/AREVA GDA Task Analysis: Entry into the Severe Accident management Guidelines (OSSA)	71
GI-UKEPR-HF-01.A1	D2.5 R7 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0007-D-BPE	EDF/AREVA Task Analysis: Primary Circuit depressurisation in the EOP and OSSA	72
GI-UKEPR-HF-01.A1	D2.5 R8 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0008-D-BPE	EDF/AREVA Task Analysis: Operator Responses to Loss of Instrumentation and Control [OP_EFWS]	73
GI-UKEPR-HF-01.A1	D2.5 R10 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0010 Issue E-BPE	EDF/AREVA GDA Task Analysis: Operator Response to decreasing RCS Level [OP_SIS_INJ_80MN_NCSS] on the Non Computerised Safety System	74
GI-UKEPR-HF-01.A1	D2.5 R10 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-000-RPT-0010 Issue G-BPE	EDF/AREVA GDA Task Analysis: Operator Response to decreasing RCS Level [OP_SIS_INJ_80MN_NCSS] on the Non computerised Safety System	75

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A1	D2.5 R10 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	EDF Note ECUK121139, Rev. A	EPR UK GDA – Human Factors – Time estimate for transfer to NCSS	76
GI-UKEPR-HF-01.A1	D2.5 R11a (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-0000-RPT-0024, Issue D-BPE	EDF/AREVA GDA Task Analysis: NCSS Action for OP_BLEED_30MN_NCSS	77
GI-UKEPR-HF-01.A1	D2.5 R11b (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	16895-707-0000-RPT-0011, Issue D-BPE	EDF/AREVA GDA Task Analysis: NCSS Action for [OP_EFW_NCSS], [OP_FB_120M_MDEP_NCSS], [OPE_52_LOCAL], [OP_SBODG_LOCAL]	78
GI-UKEPR-HF-01.A1	D2.5 R13 (not individually listed within Resolution plan but will form part of overall D2.5 deliverable)	PEPSF/12.104 Rev 1	GI-UKEPR-HF-01 – Confirmation of Design Features Related to Claims M3/M23/M25/M28	79
GI-UKEPR-HF-01.A1	D2.5	16895-707-000-RPT-025, Issue C-BPE	EDF/AREVA GDA Task Analysis Summary Report	80
GI-UKEPR-HF-01.A1	D3.1	16895-707-000-RPT-0015 Issue F-BPE	Holistic arguments and evidence to support claims relating to misdiagnosis in emergency operations	81
GI-UKEPR-HF-01.A1	D3.3	16895-707-000-RPT-0017 Issue G-BPE	EDF/AREVA GDA Human Factors: PICS to SICS transfer: A claims, arguments and evidence-based safety case	82
GI-UKEPR-HF-01.A2	D4.1	16895-707-000-RPT-0018, B-PREL	EDF/AREVA GDA Human Factors: PCSR Sub-Chapter 18.1 Revised Structure	83
GI-UKEPR-HF-01.A2	D4.1	UKEPR-0002-181, Advance Version of Issue 06	PCSR Sub-Chapter 18.1 - Human Factors	84

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0– Identification & Substantiation of Human Based Safety Claims – EDF and AREVA Deliverables

GDA Issue Action	Human Factors Topic	Document Ref.	Title	Ref.
GI-UKEPR-HF-01.A2	D4.1	UKEPR-0002-181, Issue 06	PCSR Sub-Chapter 18.1 - Human Factors	85

GI-UKEPR-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims – Regulatory Comment Letters Provided

Letter Reference	GDA Issue Action	Subject
EPR70335R	A1	EDF/AREVA GDA Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors
EPR70336N	A1	EDF/AREVA – GI-UKEPR-HF-01 Deliverable D2.2 – Schedule of intermediate Type C Task Analyses – ONR comments
EPR70342R	A1	ONR Comments on GI-UKEPR-HF01 Deliverable D2.5 - EDF/AREVA Task Analysis: Feed and Bleed Recovery
EPR70340R	A1	UK GDA Analysis of pre-initiator Human Errors - Risk Significant Equipment Grouped by Generic Equipment Type (including Legacy - Non Legacy Status)
EPR70341R	A1	UK EPR™ - Identification and categorisation of PSA 2011 type C claims, PEPSPF/11.304
EPR70371R	A1	EDF/AREVA GDA Task Analysis Methodology; Analysis of Type A and B Pre-fault Human Errors arising from Maintenance, Testing and Calibration – Final Issue report and response to ONR Comments
EPR70378R	A1	GI-UKEPR-HF-01/A.1 /Deliverable D1.8 'Dropped loads and fuel handling: Methodology for the identification of Human Based Safety Claims' PEPS-F DC 96 Rev B. – ONR Comments
EPR70383N	A1	GI-UKEPR-HF-01/A.1 – UK GDA Analysis of pre-initiator Human Errors – Risk Significant Equipment Grouped by generic Equipment Type

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims – Regulatory Comment Letters Provided

Letter Reference	GDA Issue Action	Subject
EPR70384N	A1	EDF/AREVA GDA resolution Plan GI-UKEPR-HF-01 – Planned deliverable D2.5 Intermediate submission of substantiation of Type C HFEs' – No longer required
EPR70392N	A1	GI-UKEPR-HF-01/A.1 – Response to ONR Comments on Deliverable 2.5 – EDF/AREVA Task Analysis: Feed and Bleed Recovery
EPR70394N	A2	GI-UKEPR-HF-01 – ONR comments on EDF/AREVA GDA Human Factors: PCSR Sub- Chapter 18.1 Revised Structure
EPR70395N	A1	GI-UKEPR-HF-01/A.1 – Heterogeneous Dilution – Methodology Report
EPR70396R	A1	GI-UKEPR-HF-01 – ONR comments on PEPSPF/11.486 Rev 1 Confirmation of design features relating to misalignment of automated valves
EPR70403N	A1	GI-UKEPR-HF-01/A.1 – Deliverable D1.9 Dropped Loads and Fuel Handling – Risk Analysis Methodology - ONR comments
EPR70406R	A1	GI-UKEPR-HF-01/A.1 – Deliverables D1.3 Identification of tasks associated with Type A/B Human failure Events, Modelled in the PSA and D1.4 Task Analysis (Human HAZOP) Programme for Type A/B Human Failure Events Modelled in the PSA - ONR comments
EPR70409R	A1	GI-UKEPR-HF-01/A.1 – Deliverable D2.5 – Post Fault Task Analysis of Claim H2 – ONR comments
EPR70412R	A1	GI-UKEPR-HF-01 – ONR Response to letter EPR01123R on Confirmation of design features related to claims M3/M23/M25/M28
EPR70413R	A1	GI-UKEPR-HF-01– Deliverable D2.3 – Steam Generator Tube Rupture Recovery Strategies Post – ONR comments
EPR70424R	A1	GI-UKEPR-HF-01 – ONR Response to letter EPR01166R and Deliverable D2.5 R10 Task Analysis of Claim H8 - Operator response to decreasing RCS Level (OP_SIS_INJ_80MN_NCSS) on the Non Computerised Safety System
EPR70423R	A1	GI-UKEPR-HF-01 – ONR Response to letter EPR01164R and Intermediate Deliverable D1.5 – Substantiation of Identified Type A Human Failure Events Modelled in the PSA
EPR70429R	A1	GI-UKEPR-HF-01 – ONR Response to letter EPR01217R and Deliverable D2.4 Human Factors: Internal Flooding

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims – Regulatory Comment Letters Provided

Letter Reference	GDA Issue Action	Subject
EPR70427R	A1	GI-UKEPR-HF-01/A.1 – Deliverable D2.5 R4 – Task Analysis of Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M] – ONR comments
EPR70432R	A1	GI-UKEPR-HF-01 – ONR Response to letters EPR01224R / EPR01248R and Deliverables D1.10a Identification of Dropped Loads and Fuel Handling Human Based Safety Claims – Polar Crane and D1.10b Identification of Dropped Loads and Fuel Handling Human Based Safety Claims – Refuelling Machine
EPR70433R	A1	GI-UKEPR-HF-01 – Amendment to ONR Letter EPR70429R on Human Factors claims relating to Internal Flooding
EPR70434R	A1	ONR treatment of initial submissions for Close-out of GI-UKEPR-HF-01

GI-UKEPR-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1479	A1	Various	Request for English versions of French documents referenced in the response to TQ-EPR-1026 that was raised during GDA Step 4 to query EDF and AREVA's approach to Human Factors Integration
TQ-EPR-1505	A1	PEPS-F DC 96 Rev. B	Various queries seeking clarification and additional information related to the methodology to be followed by EDF and AREVA when identifying potential human errors that will result in dropped loads
TQ-EPR-1526	A1	ECEGIG111647 A	Various queries regarding the claims made on operators with regard to the mitigation of internal flooding events.
TQ-EPR-1552	A1	16895-707-000-RPT-0014 BPREL	Queries on the completeness of the methodology document provided for the analysis of potential human errors related to Heterogeneous Boron Dilution and the provision of referenced documents.

Annex 1

Deliverables and Associated Regulatory Comment Letters and Technical Queries Raised During Close-out Phase

GI-UKEPR-HF-01 Revision 0 – Identification & Substantiation of Human Based Safety Claims – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1556	A1	PEPSPF/11.486 Rev. 1	Request for particular reference noted within the submission
TQ-EPR-1600	A1	Various	Various queries relating to the treatment of Issues and Assumptions arising from the work to Close-out GDA Issue GI-UKEPR-HF-01 by EDF and AREVA; in particular how identified issues and assumptions are being captured and managed to ensure that they can be suitably addressed by a future licensee.
TQ-EPR-1600	A1	UKEPR-I-042 Rev. 01	Human Factors Tracking Registers – details the process and final HF Issues and Assumptions from the work undertaken to address GDA Issue GI-UKEPR-HF01.

Annex 2

GDA Assessment Findings Arising from GDA Close-out for Human Factors GDA Issue GI-UKEPR-HF-01

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-HF-55	The Licensee shall ensure that its operating philosophy is consistent with the assumptions made in the GDA HF substantiations on the use of the SOA approach, procedures, and on the key operating roles of Action and Strategy Operators (OA and OS), the Safety Engineer (SE) and Field Operator (FO). If an alternative approach is intended by the licensee then re-justification of all relevant HBSCs will be required and re-analysis as necessary.	Prior to First structural concrete
AF-UKEPR-HF-56	The Licensee shall determine the impact of credible degradation and failure modes of the C&I systems on the PICS displays and their resulting impact on any claimed operator actions. The licensee will need to re-substantiate any affected HBSCs.	Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-UKEPR-HF-57	The Licensee shall determine the most effective use and presentation of alarms to support claimed operator actions during SOA and OSSA operations. This shall include consideration of the use of the Plant Overview Panels as a means of displaying alarms and how any specific alarm monitoring should be included in SOA operation by both the OA, OS team and the SE.	Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-UKEPR-HF-58	The Licensee shall determine if internal floods generate additional alarms that are likely to mask or delay response to key alarms or indications prompting operators to undertake claimed leak response actions. The licensee shall provide an appropriate justification that any claimed operator actions required to support the Internal Hazards flooding case are reliably achievable within the required timescales.	Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-UKEPR-HF-59	The Licensee shall provide further substantiation for PICS to SICS transfer and the time required to start reliable SICS (or NCSS) panel operation. It shall also justify that operating roles from the SICS panel can provide the most effective approach for operation from the SICS panel.	Prior to Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 2

GDA Assessment Findings Arising from GDA Close-out for Human Factors GDA Issue GI-UKEPR-HF-01

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-HF-60	The Licensee shall address and implement all the items identified from the GDA HF assessments in the HF Issues and Assumptions Registers, or provide a justification for any alternative position taken on any given item. It should also provide ONR with a programme showing where and when in its future work it envisages addressing each HFIR item and HFAR assumptions.	Prior to First structural concrete

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

Annex 3

GDA Issue, GI-UKEPR-HF-01 – Human Factors – UK EPR™

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

IDENTIFICATION & SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS

GI-UKEPR-HF-01 REVISION 0

Technical Area	**HUMAN FACTORS**		
Related Technical Areas	Probabilistic Safety Assessment Internal Hazards Fault Studies		
GDA Issue Reference	**GI-UKEPR-HF-01**	**GDA Issue Action Reference**	**GI-UKEPR-HF-01.A1**
GDA Issue	Inadequate substantiation of human based safety claims and omission of a consolidated Human Factors safety case for the UK EPR		
GDA Issue Action	Substantiate the UK EPR™ human based safety claims. It is the expectation of ONR that all human based safety claims are considered along with supporting holistic arguments for key elements of the proposed UK EPR™ design and operation. It will be necessary to complete the identification of UK EPR™ human based safety claims. Human based safety claims may also result from safety analysis undertaken in related technical areas; principally Internal Hazards and Fault Studies. It will not be sufficient to only consider claims currently modelled in the PSA. All identified actions should be sentenced; however it will not be necessary to fully analyse in detail all individual claims. Our expectation is that the substantiation is both targeted and proportionate; recognising the human contribution to overall risk. Sentencing may employ an initial risk based screening of actions, but consideration should also be given to task complexity and novelty, and to UK EPR™ specific issues. In particular the response should include: • Substantiation of the Type A and B human failure events (HFEs). - Submit a methodology for the substantiation of Type A and Type B. - Complete the identification of Type A HFEs. - Substantiate the identified Type A HFEs on the basis of system contribution to overall risk, and proportionate contribution of human error to system unavailability. The selection of actions and sample size should be substantiated. - Substantiate the identified Type B HFEs and justify any sampling of actions. • Substantiate the Type C HFEs. - Advise ONR of any amendments to the methodology for the substantiation of Type C HFEs and highlight how it accommodates violation potential. - Identify additional human based safety claims arising from safety analysis undertaken in response to GDA Issues in related technical areas. - Provide targeted and proportionate substantiation of identified human actions. The sample size and type should be justified.		

Annex 3

GDA Issue, GI-UKEPR-HF-01 – Human Factors – UK EPR™

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

IDENTIFICATION & SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS

GI-UKEPR-HF-01 REVISION 0

Technical Area	**HUMAN FACTORS**		
Related Technical Areas	Probabilistic Safety Assessment Internal Hazards Fault Studies		
GDA Issue Reference	**GI-UKEPR-HF-01**	**GDA Issue Action Reference**	**GI-UKEPR-HF-01.A1**
	• Provide holistic arguments for key elements of the proposed UK EPR™ operation. - Provide arguments and evidence to support the claim that the State Orientated Approach and Automatic Diagnosis reduces misdiagnosis potential; - Provide arguments and evidence relating to situations with failed Automatic Diagnosis; and - Consider whether other holistic arguments / evidence are required to support the safety case for Human Factors. • Provide analytical evidence on how the design of the UK EPR™ prevents and mitgates violation potential. - Submit a methodology for the substantiation of Type A and Type B HFEs that accommodates consideration of violation potential; - Provide additional evidence on how the UK EPR™ design prevents / mitigates violation potential With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

GDA Issue, GI-UKEPR-HF-01 – Human Factors – UK EPR™

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

IDENTIFICATION & SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS

GI-UKEPR-HF-01 REVISION 0

Technical Area		**HUMAN FACTORS**	
Related Technical Areas		Probabilistic Safety Assessment Internal Hazards Fault Studies	
GDA Issue Reference	**GI-UKEPR-HF-01**	**GDA Issue Action Reference**	**GI-UKEPR-HF-01.A2**
GDA Issue Action	Provide a consolidated HF safety case and PCSR update for the UK EPR. EDF and AREVA should provide an updated PCSR submission that presents the overall HF safety case for the UK EPR. This should include and integrate the various submissions stemming from work undertaken during GDA and that related to action GI-UKEPR-HF-01.A1. With agreement from the Regulator this action may be completed by alternative means.		

Annex 4

Assessment Summary for Type C Substantiations

This annex provides a summary of ONR's assessments of the post-fault Type C HFEs submissions provided by EDF and AREVA as part of the GDA Issue **GI-UKEPR-HF-01** Close-out programme along with those that have contributed to GDA issues from other technical areas.

The HFIR numbers given in the summaries use those given in the specific submission. These should be used when considering the HF item identified.

1. Type C Human Failure Events Modelled in the Probabilistic Safety Assessment

Document Title:	**EDF/AREVA GDA Task Analysis: Feed and Bleed Recovery Strategies (OP_BLEED120MN; OP_BLEED_30MN)**	
Document No:	AMEC Report 16895-707-000-RPT-0001, Issue E-BPE, Oct 2011 TRIM ref. 2011/609984	
PSA nomenclature:	OP_BLEED120MN OP_BLEED_30MN	HEP = 8.12×10^{-3} HEP = 1.01×10^{-1}
Claim description:	This TA report covers several bleed/feed actions in differing scenarios. Two key scenarios have been selected as both representing the key demands for operator actions; and including the high risk scenario specifically. OP_BLEED120MN – this is demanded following a Loss of Main Feed Water with failure of the Start-up and Shutdown Feedwater system and common cause failure on the Emergency Feedwater System (EFWS). OP_BLEED_30MN – the actions are as for the 120 minute scenario; this is claimed following a small break Loss Of Coolant Accident (LOCA) with failure of the Main Steam Bypass and Main Steam Relief Train.	
Timescales:	2 hours; and 30 minutes respectively	
Risk Importance:	OP_BLEED_120MN – high OP_BLEED_30MN – medium	
Personnel:	OA, OS for both scenarios	
Summary of EDF/AREVA Analysis: Adequacy of substantiation	EDF and AREVA consider the OP_BLEED_120MN claim to be substantiated if the HFIR items are addressed. EDF and AREVA judge that there is considerable uncertainty over OP_BLEED_30MN; and that the key issue is when a sufficiently compelling cue is provided to the operators to initiate	

Annex 4

Assessment Summary for Type C Substantiations

	Feed and Bleed actions.
HFIR items – number & nature	044, 045 – for specific procedure requirements 046, 047 – for the need for compelling cue to start Bleed and Feed for both claims 048 – over uncertainty with the timescale (assessed and available) & whether the task can be performed within 30 minutes
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim	The assessment has been detailed, thorough and addressed all key HF issues. The conclusions made by EDF/AREVA are appropriate. Both claims require the identified HFIR items to be addressed in order for them to be fully substantiated.
Degree of substantiation:	Partial – for both claims
Key issues noted:	HMI for compelling cues for Bleed and Feed actions Need to address specific procedures issues identified by HFIR items. 30 minute claim no longer appears in the risk significant listing of operator actions in the revised PSA – replaced by another claim within 30 minutes from the NCSS; reduced reliability HEP = $3.96e^{-01}$
Key issues for further consideration:	The identified HFIR items arising from this TA need to be addressed by a future licensee.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis of Post Fault Claim H2 [OP_LHSI_IND_120MN]**	
Document No:	AMEC Report 16895-707-000-RPT-0003, Issue G-BPE, October 2012 TRIM Ref 2012/408990	
PSA nomenclature:	OP_LHSI_IND_120MN	HEP: 2.13×10^{-3}
Claim description:	This claim is required in fault scenarios with a Loss of Ultimate Heat Sink or a Total Loss of Cooling Chain when in plant state D. The claim is for the operator (failing) to start the Low Head Safety Injection (LHSI) independent of Component Cooling Water System (CCWS) / Essential Service Water System (ESWS) within 2 hours when the plant is in plant state D with the Reactor coolant System (RCS) inventory at mid-loop level.	
Timescales:	120 minutes post-fault.	
Risk Importance:	High (RIF=17.9; FV=3.6×10^{-2})	
Personnel:	OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information	
Summary of EDF/AREVA Analysis: Adequacy of substantiation	EDF/AREVA judge that the claim is substantiated due to: – The task being a simple MCR execution – It is in response to a clear challenge to a key CSF – There is a large margin between the assessed time (64.5 minutes) and the required time.	
HFIR items – number & nature	None identified.	

Annex 4

Assessment Summary for Type C Substantiations

Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim	ONR considers that this claim has been adequately substantiated at this point in the design & safety case development. The analysis has been detailed and identified all key PSFs influencing task performance and reliability. This claim is reliant on timely recognition of the need for LHSI manual start which is reliant on: – The AD and SOA approach to take the OA to the appropriate response procedure – The quality of both the SOA and detailed OA procedure – The detailed HMI displays that interact with the procedures The assumptions made about these for this assessment are consistent with ONR's GDA Step 4 HF findings and are judged to be appropriate.
Degree of substantiation:	Partially – primarily due to the reliance on assumptions
Key issues noted:	Implementation/consideration of key assumptions required by a future licensee.
Key issues for further consideration:	As above

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**AMEC Report EDF/AREVA GDA Task Analysis of Post Fault Claims M2 [OP_EFW/MSRT_2HLOCAL] and M7 [OP_SBODG30M]**	
Document No:	16895 -707-000-RPT-0004, Issue F-BPE, October 2012 TRIM Ref 2012/436940	
PSA nomenclature:	OP_EFW/MSRT_2HLOCAL OP_SBODG30M	HEP: 5.0×10^{-2} HEP: 4.28×10^{-2}
Claim description:	OP_EFW/MSRT_2HLOCAL – the operator fails connect the local cross-connection of the EFW line and initiation of secondary cooldown within 2 hours. The claim is in response to a Loss of Off-site power and to prevent RCP pump seal damage leading to a LOCA. ***This is claim M2.*** OP_SBODG30M – the operator fails to start the Station Blackout (SBO) Diesel Generators (DGs) within 30 minutes. It is a required post fault response to a Loss Of Offsite Power (LOOP) (incidental conditions) with failure of the a Stand Still Seal System (SSSS) leading to a LOCA due to a leak at RCP seals (e.g. accidental conditions; which are entered, with SI activation, 9.5 minutes after the LOOP). ***This is claim M7.*** As the initiating event for both claims is a LOOP, many of the actions required in M2 are required in M7. Achievement of the claim in M2 however involves an initial response to a LOOP then implementation of cooling (the success criteria) after cross connection of the EFWS injection lines to ensure water supply to all the SGs by available EFWS pumps.	
Timescales:	133 minutes and 30 minutes respectively	
Risk Importance:	Medium (complex)	
Personnel:	OP_EFW/MSRT_2HLOCAL – requires both MCR actions by OA and LTP actions by an FO OP_SBODG30M – MCR actions only by OA	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	OP_EFW/MSRT_2HLOCAL – the assessment indicates a task time of 132 minutes but states that this is considered to be conservative due various conservatisms used in the assessment. The report identifies several measures that could be used to reduce the task time, most notably automation of the EFWS header valves to remove the requirement for LTP actions. This would substantially reduce the time required. OP_SBODG30M – the assessment indicates a task time of 17 minutes. EDF/AREVA judge that the analysis substantiates the claim.
HFIR items – number & nature	HFIR items 58-65 (64 not used) These HFIR items cover: – Detailed aspects of the HMI; notably on EFWS efficiency and a response to it to ensure timely overall response – Detailed aspects of both the SOA and MOP procedures to ensure that operators are taken to, and alerted to the need to take particular actions – Consideration of the complexity of LTP actions – and the allocation of work between OS and SE to address this – Measures to reduce the time required for claim M2; most notably to automate the EFWS valves so removing the need for LTP action[13]

[13] These EFWS valves have been automated subsequent to the analysis as part of GDA design changes.

Annex 4

Assessment Summary for Type C Substantiations

Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The TA has been thorough and identified all key issues. It does rely on several assumptions on SOA operating practices and on SME judgements (particularly over timescales). ONR considers that the uncertainty over execution timescales for M2 indicate that sufficiently reliable manual operation can only be assured by the automation of the EFWS valves removing the need for LTP actions. At first sight this would appear to be the most appropriate ALARP option. The analysis and ONR assessment indicate that careful consideration needs to be made on developing procedures & their interaction with HMI details to ensure key actions are recognised and achieved in timescales required by the safety case. Overall it appears that reliable manual start-up of the SBO DGs should be achievable within the 30 minutes required period. This is borderline against the general '30 minute rule' expectation and so an ALARP case would need to be made as to why it is required.
Degree of substantiation:	Partially – for M2; Fully for M7
Key issues noted:	As HFIR noted items.
Key issues for further consideration:	All HFIR items need to be considered by a future licensee. Claim M7 needs to be reviewed and a revised valid claim made based on the outcome of resolution of the HFI items.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Operator responses to decreasing RCS level (OP_SIS_INJ_80MN_NCSS) on the Non Computerised Safety System**	
Document No:	AMEC Report 16895-707-000-RPT-0010, Issue G-BPE, October 2012 TRIM Ref. 2012/426247	
PSA nomenclature:	OP_SIS_INJ_80MN_NCSS	HEP: 8.44×10^{-3}
Claim description:	The transfer to NCSS operation is common to all NCSS claims; this H8 claim is high risk. The most frequent scenario containing H8 is where the SPPAT2000 is lost, but the TXS platform is still operational. The scenario corresponds to a level decrease in the RCS, following a voluntary action to lower the level in shutdown state (to reach ¾ loop operation). There will be no automatic isolation of the Chemical and Volume Control System (CVCS) letdown line by the PS due to failure of the corresponding loop level sensors. The SPPA-T2000 failure is assumed to occur immediately after the Initiating Event (IE), leading to failure of diversified automatic isolation. However, an automatic isolation of the CVCS letdown line will be carried out by the NCSS. Then, the required operator action is to start LHSI, using the NCSS platform.	
Timescales:	80 minutes	
Risk Importance:	High	
Personnel:	MCR operators (OA, OS), SS, SE – main tasks performed by OA and OS with the SS and SE potentially giving additional error recovery potential.	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	Due to the lack of detailed information on the NCSS system the analysis uses some assumptions about the NCSS and fault scenario: – The NCSS operates via the SICS interface (a sub-set) – There is no automatic isolation of the CVCS letdown by the NCSS The TA use other key assumptions: – Operators are well trained and familiar with PICS to SICS transfer and NCSS actions – Transfer to NCSS operation requires two switches to be turned that are on the SICS panel; one to activate the SICS panel controls; the other to enable NCSS operation – The PSIS provides a 'life sign' that indicates PICS failure – a clear, compelling visual and acoustic alarm will alert the operators to the need to undertake the transfer to NCSS operation EDF and AREVA assess the transfer time for NCSS operation to be 15 minutes, and the total task time for H8 as being 42 minutes. The analysis acknowledges that it is based on many assumptions that need to be implemented for the claim to be valid. EDF and AREVA have provided EDF N4 operational experience to support the 15 minutes transfer time. This indicates that the assessed time is likely to be conservative for situations with clear PICS failure.
HFIR items – number & nature	HFIR items 89-92. These identify specific issues that need to be considered in developing the detailed design and supporting procedures for transfer to, and operation via the NCSS system.

Annex 4

Assessment Summary for Type C Substantiations

Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The assessment has been thorough as is possible at this stage of the NCSS design; the assumptions used are appropriate; and the HFIR items encompass all key issues arising from this claim. However I would have expected more detailed information to normally be available for such an important safety system and HMI at this point in the development of the UK EPR. The assessed transfer time for NCSS operation (15 minutes) appears to be feasible in scenarios that are very clear and 'stark' to the operators. I judge that a longer timescale may be required for any scenarios where the PICS failure is via progressive degradation rather than clear failure. Consultation with my C&I colleagues indicates that the presentation of failure modes of PICS have not been clearly determined at GDA. The margin between the assessed time and required time does appear sufficient to potentially support the H8 claimed reliability. However the issues identified in the HFIR need to be addressed in order to support this claim adequately.
Degree of substantiation:	Partially.
Key issues noted:	As HFIR noted items.
Key issues for further consideration:	All HFIR items need to be considered by a future licensee. The timescale for reliable transfer to the NCSS needs further substantiation post-GDA to ensure that all PICS degradation and failure modes are encompassed.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies Post fault task analysis of "SGTR 1 tube" and claims OP_SCD_30MN and OPE_SGTR**	
Document No:	AMEC Report 16895-707-000-RPT-0002, Issue I-BPE, October 2012	
PSA nomenclature:	SGTR 1 tube OP_SCD_30MN OPE_SGTR – HEP	HEP: no explicit HEP HEP: 4.28×10^{-2} HEP: 1×10^{-4}
Claim description:	SGTR 1 tube – this supports the SGTR position reflected in the formal Change Management Form (CMF) UKEPR-CMF-022 and cited as option 1 in PEPR-F DC 38. This uses N16 sensors to detect SG leaks less than 1 tube diameter double ended break, and then requires manual cooldown and reactor trip. OP_SCD_30MN – claim M15. Initiation of secondary cooldown within 30 minutes of an SI signal for >1 SG tube failures OPE_SGTR – HEP – claim H7. Initiation of partial cooldown for scenarios with a steam line break and induced 2 tube SG failure before the In-Containment Refuelling Water Storage Tank (IRWST) empties (at least 12 hours available).	
Timescales:	For SGTR 1 tube the time is 50 minutes. For OP_SCD_30MN (claim M15) the time is 30 minutes; For OPE_SGTR – HEP – there is at least 12 hours for primary to secondary leak isolation, with secondary cooldown initiation being required within 4 hours.	
Risk Importance:	SGTR 1 tube is taken as being equivalent to high risk – due to its importance to the deterministic safety case requirements. OP_SCD_30MN is medium; OPE_SGTR – HEP is high.	
Personnel:	All safety claimed tasks in these three claims are MCR actions; personnel are: OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	A detailed TA has been performed for all 3 claims with particular attention placed on the timeline assessments for the SGTR 1 Tube and OP_SCD_30MN. For STGR 1 tube the assessed time is well within the 50 minute requirement for reactor trip and complete isolation of the affected SG being around 15 minutes later. EDF/AREVA have identified several procedural and HMI issues that should be addressed to ensure that all desired operator actions can be completed more assuredly within the required 50 minutes. For OP_SCD_30MN the assessed time is 52 minutes and even allowing for conservatisms in the analysis EDF/AREVA conclude that this task is not substantiated. It is envisaged that the transient analysis determining the time requirements is very conservative; and that procedure and HMI details can be revised to ensure reliable task completion on a considerably shorter timescale. Additionally an inexperienced operator was used in the simulation studies and EDF and AREVA judge that the times generated are very conservative. EDF/AREVA judge that this claim can be supported with revised transient analysis and addressing noted HMI and procedure issues. For OPE_SGTR – HEP assess that there are very large time margins for the execution of both secondary cooldown initiation (44 minutes vs. 4 hours) and leak isolation (6 hours vs. >12 hours). Several detailed HMI and procedural issues have been identified but EDF/AREVA judge on the basis these will be addressed the claim is fully supported.
HFIR items – number & nature	Seven HFIR items are identified. HFIR items 050-054 – these are detailed HMI and procedural issues that need to be addressed to ensure that the key required actions are more reliably completed within the required safety case timescales. HFIR items 167 & 168 – these stem from further consideration of LTP actions. 167 is for provision of clear feedback to the FO for SGBS valve alignment; 168 is on valve height position to ensure it matches HF requirements.

Annex 4

Assessment Summary for Type C Substantiations

Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. For SGTR 1 tube ONR considers that manual trip and SG isolation can be reliably achieved within the necessary 50 minute timescale if the identified HMI and procedural issues are adequately addressed. The acceptability of reliance on manual actions for the deterministic case for SGTR protection is considered further in GDA Issue GI-UKEPR-FS-04. For claim OP_SCD_30MN (claim M15) – ONR does not consider that this claim is supported. A valid claim may be possible but only if the timescale is extended and/or the identified procedure and HMI changes then robustly show that the operator actions can be reliably achieved within the 30 minute timescale. For OPE_SGTR – HEP (claim H7) – ONR considers that this claim is adequately supported if the identified issues are addressed.
Degree of substantiation:	SGTR 1 tube – Partially OP_SCD_30MN – Not at all unless HFIR items 50-54 are addressed OPE_SGTR – HEP Partially
Key issues noted:	Detailed HMI and procedural issues need to be addressed for each of these claims to be valid. The main issues are: – Ensuring the detailed HMI provides timely, compelling cues for key actions – Ensuring detailed aspects of both SOA and MOPs are appropriately sequenced, and include specific instruction/guidance to ensure key actions are identified and achieved within the necessary timescales
Key issues for further consideration:	See HFIR items noted above.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK]**	
Document No:	AMEC Report 16474-TR-006, Issue G-PDE, May 2012 TRIM Ref. 2012/206357	
PSA nomenclature:	OP_FEED_TK	HEP: $1x10^{-4}$
Claim description:	The claim OP_FEED_TK is defined as 'The operator cross connects the EFWS tank and re-feeds the Start-up and Shutdown System (SSS), Main Feedwater System (MFWS) or the EFWS tank.' The claim covers a variety of scenarios with differing numbers of trains of EFWS available. The highest risk scenario is for a Loss of Ultimate Heat Sink with all 4 EFWS trains available.	
Timescales:	There are 2 key essential elements: – Cross-connection of the EFWS tanks – Provide longer term inventory by connecting the EFWS tanks to the fire-fighting system at 24 hours The initial key task is required within 4 hour time period.	
Risk Importance:	High; RIF=350.3; FV=$3.5x10^{-2}$	
Personnel:	This claim is reliant on MCR monitoring to determine the need for actions; and LTP action for the cross-connection and make-up: OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information FO – to implement the LTP actions	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	This is an update of the assessment presented at GDA Step 4. The revised report responds to comments made in the GDA Step 4 HF Assessment report (Ref. 7). The analysis indicates that there is a large margin for task execution (39mins for EFWS cross-connection; 83mins for make-up against 4 hours and 24 hours respectively). The analysis indicates that task reliability is very dependent on monitoring of plant status and the HMI alerting the operators of the need for the two key tasks. The assessment considers the claim is not adequately supported unless identified HMI and procedural issues are addressed. These relate primarily to ensuring that a clear and compelling cue is provided to the operators to alert them for the need for the cross-connection and make-up tasks. Additionally consideration should be made to automating the key local to plant actions.
HFIR items – number & nature	HFIR items 032-044 and 082
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. This revision has addressed ONR's comments made at GDA Step 4 and now acknowledges the need to address the HMI and procedural issues identified.
Degree of substantiation:	Partially
Key issues noted:	The lack of compelling cues to the operator for the two key tasks on the HMI overview display used for routine monitoring. Enhanced procedure guidance. Consideration of automation of the LTP actions – for ALARP.
Key issues for further consideration:	As HFIR items noted above.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims**	
Document No:	AMEC report 16474/TR/003 D-BPE, May 2012, TRIM Ref. 2012/224378	
PSA nomenclature:	OP_SBODG2H OP_FSCD_30MIN	HEP: 2.13×10^{-3} HEP: 4.28×10^{-2}
Claim description:	OP_SBODG2H – Operator starts up the SBO DGs remotely from the MCR following a LOOP and failure of the Emergency Diesel Generators (EDGs). OP_FSCD_30MIN – following a small break LOCA a partial cooldown is initiated automatically on the SI signal. All Medium Head Safety Injection (MHSI) trains are unavailable; the operator manually initiates a cooldown once partial cooldown is completed, to reach LHSI system injection pressure and control RCS inventory. The PSA nomenclature indicates manual initiation of fast cooldown. The TA indicates that fast cooldown is not required. A controlled cooldown at $50^{o}Chr^{-1}$ is the requirement.	
Timescales:	OP_SBODG2H – 1.5 hours to prevent SG level falling below 14% (and changing scenario) OP_FSCD_30MIN – 30 minutes for worst case RCP seal LOCA scenarios; longer timescales up to 90 minutes for $2cm^2$ LOCA.	
Risk Importance:	OP_SBODG2H – High; RIF =14.6; FV = $2.91E^{-02}$ OP_FSCD_30MIN – High; RIF =3.9; FV = $1.28E^{-01}$	
Personnel:	MCR actions only for both claims OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	A detailed TA has been performed for both claims. OP_SBODG2H – the analysis shows that is a large margin for action (32 minutes assessed time vs. 90 minutes requirement). Some specific HMI and procedural improvements have been identified, but overall EDF/AREVA judge the claim to be adequately supported. OP_FSCD_30MIN – the assessed time is longer than that required (38 minutes assessed); hence it is judged that the claim is not supported at this point. Additionally the analysis has identified various potential errors that could delay task execution. EDF and AREVA conclude that they judge the claim can be supported if the identified procedure and HMI issues are addressed. EDF and AREVA judge that a modified valid claim can be supported – this will require: – Altering the task requirements – changing the action from controlled to fast cooldown, and amending the scenario timescale to 40 minutes by reducing conservative bounding used in the PSA) – Addressing specific HMI and procedure issues identified in the analysis (& included in the HFIR).
HFIR items – number & nature	OP_SBODG2H – 13 HFIR items are identified. OP_FSCD_30MIN – 2 HFIR items are identified. Most of these items relate to: – Specific HMI details – Specific procedure issues (for sequencing & reliable task need recognition) – for both SOA paper procedures and computer presented MOPs
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	This assessment is an update of that presented at GDA Step 4 – and addresses the detailed comments made in the GDA Step 4 HF Assessment report (Ref. 7). EDF and AREVA have addressed all the comments made. For OP_SBODG2H the claim appears to be readily ‘substantiatable’. For OP_FSCD_30MIN there is considerably more uncertainty whether a valid claim bounding all necessary scenarios can be supported. However this analysis does indicate that a valid claim should be possible for at least the majority of PSA scenarios where this claim is included.

Annex 4

Assessment Summary for Type C Substantiations

Degree of substantiation:	OP_SBODG2H – Partially OP_FSCD_30MIN – Not at all
Key issues noted:	These are as captured by the HFIR items.
Key issues for further consideration:	OP_SBODG2H – the HFIR items need to be addressed to match ALARP expectations and to fully substantiate the claim. OP_FSCD_30MIN – this needs to be reviewed and amended in conjunction with the PSA model in order to produce a revised valid claim. The identified HFIR items will need to be addressed as part of this amendment process.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis of Post Fault Claims M6, M8 and M19**	
Document No:	AMEC report 16895-707-000-RPT-0005 D-BPE, September 2012, TRIM Ref. 2012/391024	
PSA nomenclature:	M6 = OP_FSCD_30MN M8 = OP_52 M19 = OP_COMBI_240MN_LDEP	HEP = $1.01x10^{-1}$ HEP = $1.00x10^{-4}$ HEP = $5x10^{-2}$
Claim description:	M6 [OP_FSCD_30MN] – operator fails to initiate Fast Secondary Cooldown (FSCD) within 30mins following a seal LOCA in plant state A/B. Actual detailed claim is for operators to perform a secondary cooldown a 50C/h (requires opening of Main Steam Relief Train (MSRT) valves). Action required 30mins after SI signal. M8 [OP_52] – failure to initiate IRWST cooling with Containment Heat Removal System (CHRS) within 4 hours of reactor trip following a Loss of Ultimate Heat Sink (LUHS) from an external hazard. M19 [OP_COMBI_240MN_LDEP] – operator fails to initiate primary bleed and LHSI for injection with IRWST cooling + low dependency. It is required following a loss of RHR cooling whilst in plant state Cb (3/4 loop operation).	
Timescales:	M6 – 30 minutes from the SI signal M8 – around 7 hours post reactor trip M19 – notionally >4hours; 15 minutes from reaching key criterion for action (SG level WR<14%)	
Risk Importance:	All three are medium complex.	
Personnel:	MCR actions only for all claims: OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information However M8 can be adversely affected by a LTP FO error undertaking a procedurally required task prior to the claim action.	

Annex 4

Assessment Summary for Type C Substantiations

Summary of EDF/AREVA Analysis: Adequacy of substantiation	A detailed TA has been performed for all claims. M6 – not substantiated as time required exceeds time available; however judged that the claim is likely to be feasible with revised transient analysis (extending time) M8 – action judged as feasible and appropriate allocation of function; HFIR item 120 raised on addressing the identified LTP FO error that could prevent the claimed action being effective. M19 - action judged as feasible and appropriate allocation of function. It also identifies that the assumed dependency on a previous PSA modelled action does not exist (HFIR item 122).
HFIR items – number & nature	Four HFIR items are identified: 119 – on revision of the timescale for M6 120 – for further consideration of checks and feedback on actions that may impact on success of the claimed action 121 – conduct transient analysis to determine the timescales for SG water levels occurring in the scenario for M8 122 – review of the dependency assumed between M19 and a previously modelled PSA claimed action
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. The analysis and resulting HFIR items are appropriate.
Degree of substantiation:	For M6 – the claim is not substantiated; however EDF and AREVA's judgement appears reasonable on the timescale being conservative. Additionally the time required stems from completion of previously started MOP actions. There is potential for re-prioritising the response (based on OS and SE intervention) to ensure that the key action is undertaken. For M8 – the claim is partially substantiated. HFIR item 120 needs implementation in order to support the very high reliability claimed for M8. For M19 – partially. The uncertainty stems from the small time window assumed for successfully completing the claimed action once the criterion for action requirement is reached (10 minutes required vs. 15 minutes grace time). The time requirement appears conservative.
Key issues noted:	As above – these are all addressed by the identified HFIR items.

Annex 4

Assessment Summary for Type C Substantiations

Key issues for further consideration:	Consideration/implementation of the HFIR items.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims Primary circuit depressurisation in the EOP and the OSSA**	
Document No:	AMEC report 16895-707-000-RPT-0007 D-BPE October 2012 TRIM Ref. 2012/389245	
PSA nomenclature:	OQF-L2-DEPRESS25M (M22) OPD-L2-DEPRESSH (M24) OPD-L2- DEPRESS-40M (M21)	HEP=$5.5x10^{-2}$ HEP=$5.3x10^{-1}$ HEP=$1.5x10^{-1}$
Claim description:	The claims represent the same physical actions – depressurising the primary circuit via the Primary Depressurisation System (PDS) following a LOCA. M22 and M24 are the same action undertaken when in SOA operation – the only difference between the 2 claims is on dependency with previous operator actions. M21 is following entry into OSSA – the action is a required immediate action undertaken by the MCR staff.	
Timescales:	For M22 & 24 – there is 40 minutes from the point the action is required (106mins post-fault); execution time is 1 minute. For M21 – there are 94 minutes from the COT 650^0C OSSA entry point. Transition to OSSA operation (M16) grace time is 40 minutes.	
Risk Importance:	All medium claims.	
Personnel:	All actions are MCR actions – hence OA primarily for M22 and M24. M21 is reliant on SE recognition of OSSA entry then OA action.	
Summary of EDF/AREVA Analysis: Adequacy of substantiation	A detailed TA has been performed for all claims. For M22 and M24 the claims are assessed as having a considerable time margin (39mins) for the tasks, though an HMI improvement is identified (HFIR item 162) to improve the support to the operator for PDS 2nd line opening if the first line fails. For M21 the assessment judges that a large time margin (74 minutes) exists and the claim is an immediate one required by the OSSA procedure.	

Annex 4

Assessment Summary for Type C Substantiations

HFIR items – number & nature	Two HFIR items are identified: 159 – on review of the dependency levels and modelling for M24 and M21. 162 – on ensuring that the HMI clearly indicates when the operator is able to open valves on the PDS line.
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. The analysis and resulting HFIR items are appropriate. Claim M21 is dependent on the time for OSSA entry – see noted issue below.
Degree of substantiation:	Partially for M22 & M24 Fully for M21
Key issues noted:	The time for entry into OSSA is dependent on the time required for the SE to contact the Emergency Director (ED) and for the ED to make the OSSA entry decision. As the OSSA entry criteria are unambiguous it seems preferable for the SE to authorised OSSA entry and for immediate OSSA actions to be undertaken – with the ED being contacted for discussion on the overall OSSA strategy in parallel.
Key issues for further consideration:	Consideration/implementation of the HFIR items.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/AREVA GDA Task Analysis: Operator Responses to Loss of Instrumentation & Control [OP_EFWS] (Claim H4)**	
Document No:	AMEC report 16895-707-000-RPT-0008, Issue D-BPE, September 2012 TRIM Ref. 2012/381449	
PSA nomenclature:	OP_EFWS	HEP: 2.84×10^{-3}
Claim description:	The report covers a single claim for starting the SBO DGs then starting and manually controlling EFWS feed to the SGs following LOOP and failure of the TXS system (part of PICS platform).	
Timescales:	Transient analysis indicates 60 minutes to establish EFWS control.	
Risk Importance:	High	
Personnel:	MCR actions only for this claim: OA – to undertake the specific MCR actions OS – to maintain an overview of SOA implementation SS or SE – to provide independent monitoring of critical safety functions via the SICS panel information	
Summary of EDF/AREVA Analysis: Adequacy of substantiation	A detailed TA has been performed for this claim. This includes provision of PICS HMI screenshots for key actions encompassed by this claim. The assessment concludes that the time required to undertake the claim is longer than the required time assumed by the PSA (66 minutes vs. 60 minutes). However it is judged that the task can be made feasible and supported if three aspects are addressed: ▪ Refined transient analysis (the scenario timescales appear very conservative for many scenarios) ▪ Consideration of automation of some tasks – permitting the key task to be undertaken earlier ▪ Reconsidering task sequencing – so that EFWS control is undertaken earlier	

Annex 4

Assessment Summary for Type C Substantiations

HFIR items – number & nature	Two HFIR items are identified: 152 – relating to the AD failure; ensuring that it displays an 'invalid' message, and further consideration of failure modes and operator training for loss of TXS 165 – on the time aspects of the claim (this covers the 3 elements identified in previous section)
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. It is based on considerable assumptions about C&I failures and procedures. The analysis and resulting HFIR items are appropriate but not sufficient. It has been based on assumptions as to how the loss of TXS and C&I will occur. See noted issue below.
Degree of substantiation:	Not at all – the key C&I issues (see below) have not been adequately addressed within this assessment; and the assumptions made may not be completely valid. Key details of HMI, AoF, time requirements and procedures need to be addressed to support the claim. The analysis does suggest that for situations where loss of C&I is very evident then an acceptable claim can be supported.
Key issues noted:	There is uncertainty as to C&I failure (particularly degradation) and how this will present itself to the operators. This needs further consideration particularly on TXS failure and their potential impact on other PICS indications. At this point the assumption that the TXS failures do not impact on the MCR operator responses does not appear to be reasonable.
Key issues for further consideration:	The key issue above needs to be addressed in addition to the 2 HFIR items.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/Areva GDA Task Analysis: NCSS Action for OP_BLEED_30MN_NCSS**	
Document No:	AMEC Report 16895-707-000-RPT-0024 D-BPE, August 2012 TRIM Ref. 2012/344406	
PSA nomenclature:	OP_BLEED_30MN_NCSS	HEP: 3.96×10^{-1}
Claim description:	The report covers a single claim for initiating feed and bleed from the NCSS within 30 minutes following a fire in the Safeguard Building 1 that has caused a total loss of C&I.	
Timescales:	The time available to perform the action is 30 minutes from the Safety Injection signal which is assumed to occur at the same time as the initiating event.	
Risk Importance:	Medium	
Personnel:	MCR actions only for this claim (although it is noted that fire fighting activity will be being undertaken simultaneously it does not form part of the claim): OA – to undertake the specific MCR actions OS – to maintain an overview of corrective actions SS or SE – to provide independent monitoring	
Summary of EDF/AREVA Analysis: Adequacy of substantiation	A TA has been performed for this claim. The analysis concludes that the time required to undertake the claim aligns with the time available (30 minutes). EDF and AREVA consider therefore that the claim is achievable although they do note that no margin for error exists and record that this situation cannot be considered to be reliable and therefore should be accommodated within any further quantitative assessment of the claim. However, due to aspects such as the current limited information on the exact function and interface for the NCSS it is noted that the analysis is conservative and that this may therefore mean that less time is actually required to undertake the claimed actions. As this cannot currently be confirmed the analysis conclusions are dependent on the confirmation of the stated assumptions.	

Annex 4

Assessment Summary for Type C Substantiations

HFIR items – number & nature	One HFIR item is identified. 150 – relating to the need for supervisory personnel to address the concurrent fire incident during the first ten minutes of the scenario and therefore the need for workload during this period not be excessive in order that recovery mechanisms offered by supervisory control are still credible.
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	This analysis provides useful information on the nature of the tasks required to address the fault in the postulated conditions. However, the analysis cannot be considered to substantiate the activity any more than partially due to the lack of design detail currently available on the NCSS interface. Significant concerns also exist over the timing of the activity with respect to the time available to undertake it. EDF and AREVA have offered information that suggests that the time allowed and task times used for the analysis are conservative although this is not confirmed. The current situation, as analysed, affords no grace.
Degree of substantiation:	Partially – key details of HMI, AoF and procedures need to be developed to support the claim. The analysis has identified those issues that need to be resolved or implemented to ensure that a valid claim can be substantiated in the future. The substantiation has gone as far as it reasonably can based on the current design position.
Key issues noted:	There is a lack of design detail on the NCSS function and HMI along with concerns over the role of supervisory MCR personnel in addressing the concurrent fire. This necessitates that the analysis is based on an extensive set of assumptions, therefore negating its ability to substantiate the claim at this stage.
Key issues for further consideration:	The issue of a lack of design detail needs to be addressed along with the HFIR item that notes the role of supervisory personnel in addressing the concurrent fire.

Annex 4

Assessment Summary for Type C Substantiations

Document Title:	**EDF/Areva GDA Task Analysis: NCSS Action for OP_EFWS_NCSS, OP_FB_120M_MDEP_NCSS, OPE_52_LOCAL, OP_SBODG_LOCAL**	
Document No:	AMEC Report 16895-707-000-RPT-0011 D-BPE October 2012 TRIM Ref. 2012/414700	
PSA nomenclature:	OP_EFWS_NCSS (M9) OP_FB_120M_MDEP_NCSS (M11) OPE-52-LOCAL (M13) OP-SBODG_LOCAL (M18)	HEP = 7.74×10^{-2} HEP = 1.50×10^{-1} HEP = 5.00×10^{-2} HEP = 5.00×10^{-2}
Claim description:	The document presents the analysis of four claims, each of which is related to maintaining the cooling of the UK EPR™ post fault via the NCSS due to a Total Loss of Instrumentation and Control (TLIC) and spurious reactor trip. The different claims relate to the use of different means of cooling the plant. Two of the claims (OP_EFWS_NCSS and OP_FB120M_MDEP_NCSS) have a dependency such that latter only starts upon a realisation that the former has failed.	
Timescales:	For M9 there is 1 hour to control SG level acting on EFWS flow rate after the TLIC and spurious reactor trip. For M11 two hours are noted to be available, however it is noted that the M11 activity will only commence once M9 is considered to have failed. EDF/AREVA have analysed the nominal start point for M11 to be 1 hour after the spurious reactor trip and TLIC to take account of undertaking the M9 activity first. For M13 4 hours is available for the required activity after reaching the criteria to perform the action (T_{IRWST} reaches $100^{o}C$) which itself occurs 3 hours after the initiating event. For M18 the SBO DGs should be started by LTP action within 2 hours of the initiating event.	
Risk Importance:	All four claims analysed are of Medium importance	

Annex 4

Assessment Summary for Type C Substantiations

Personnel:	The majority of actions for all four claims are undertaken by MCR personnel within the MCR, namely: OA – to undertake the specific MCR actions OS – to maintain an overview of corrective actions SS or SE – to provide independent monitoring. FOs are involved in LTP actions to start-up the SBO DGs.
Summary of EDF/AREVA Analysis: Adequacy of substantiation	TAs have been developed for each of the 4 claimed actions under consideration. For all of the claimed actions except OP_SBODG_LOCAL EDF and AREVA conclude that the tasks required can be achieved within the available time and that the AoF is appropriate. However, in all instances the extensive use of assumptions within the analysis is noted, along with the need for these to be confirmed during the NSL phase. For OP_SBODG_LOCAL the analysis indicates that insufficient time is available to undertake the required actions. This relates to the LTP actions performed by the FO. The analysis notes that this finding means that the currently claimed HEP is not credible and that while better clarification of certain conservative assumptions may improve the situation it should also be considered whether certain tasks currently performed LTP could be undertaken from the MCR.
HFIR items – number & nature	Two HFIR items are identified. 166 – relating to the need for the NCSS functional requirements to contain a cue to determine when IRWST cooling via CHRS is required. 167 – notes specifically that the claimed operator response time for OP_SBODG_LOCAL is insufficient and that therefore the activity requires further analysis with the need to consider providing functionality within the MCR to perform some or all of the activity.
Summary of ONR Assessment: Adequacy of EDF/AREVA consideration of claim:	This analysis provides insight into the nature of the activities required to undertake the claimed human actions for each of the four HBSCs. However, the analysis cannot be considered to substantiate the claims any more than partially due to the lack of design detail currently available on the NCSS interface. Significant concerns also exist over the timing of some of the activities with respect to the time available to undertake them. This is noted by EDF and AREVA for OP_SBODG_LOCAL where insufficient time is available due to the LTP tasks required.

Annex 4

Assessment Summary for Type C Substantiations

Degree of substantiation:	Partially – key details of HMI, AoF and procedures need to be developed to support the claims. The analysis has identified those issues that need to be resolved or implemented to ensure that a valid claim can be substantiated in the future although ONR concerns remain over the timing of certain actions. The substantiation has gone as far as it reasonably can; based on the current design position.
Key issues noted:	There is a lack of design detail on the NCSS function and HMI This necessitates that the analysis is based on an extensive set of assumptions, therefore negating its ability to substantiate the claim at this stage. Further consideration is also required of the timing of some of the actions and their possible inability to be undertaken within the required timescales, particularly if the “30 minute rule” is accommodated.
Key issues for further consideration:	The issue of a lack of design detail needs to be addressed along with the timing of certain activities in order to take account of the “30 minute rule”.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

This Annex presents a summary of ONR's HF assessments that support the consideration of Dropped Loads and Internal Flooding as part of the work to Close-out Internal Hazards related GDA Issues (**GI-UKEPR-IH-01** and **GI-UKEPR-IH-03**).

The HFIR numbers given in the summaries use those given in the specific submission. These should be used when considering the HF item identified.

Internal Hazards – Dropped Loads GI-UKEPR-IH-01

ONR accepted that full identification and substantiation of HBSCs was not required for GDA as it was judged that no error reduction measures would be foreclosed at this point; the anticipated potential error defences being incorporated within detailed equipment designs (yet to be developed), and/or administrative controls.

Dropped Loads Assessment Methodology

Aims

The main purpose for the supporting HF analyses for GI-UKEPR-IH-01 is as follows:

- Identification of significant errors contributing to risk significant dropped loads;
- Identification of existing or potential error defences to prevent or reduce the likelihood of significant errors;
- Identification of mitigating actions; and
- Determination of the ALARP requirements or considerations relating to Dropped Load HFEs.

Methodology

EDF and AREVA have devised a four part process for the consideration of HBSCs for Fuel Handling Systems and Cranes for dropped load events. These parts are:

- Part 0 – selection of relevant cases
- Part 1 – Risk Analysis
    - Identification of relevant handling operations
    - Identification of critical handling operations and critical failure modes
    - Identification of failure causes of failure modes – including direct & indirect[14] human errors
    - Level of defence assessment
- Part 2 – Critical maintenance, testing and calibration tasks identification

[14] The analysis defines direct human errors as being operating or recovery action errors; indirect errors as those arising from maintenance, testing & calibration activities

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

- Part 3 – Summary of the HBSCs and consideration of the design adequacy regarding dropped loads

Only parts 0 and 1 are included in the GDA Close-out programme. Part 0 has been assessed by my Internal Hazards colleagues, so my assessment has focussed on the adequacy of Part 1 in identifying significant HFEs. EDF and AREVA's methodology uses a combination of three workshops using SMEs and design and process Failure Modes and Effects Analyses (FMEA) to undertake the analyses for the elements within the Part 1 Risk Analysis. The consequences from dropped loads are used via a severity scale to identify those tasks and failure modes judged to be of significance. The actual and potential defences against those significant HFEs are then assessed including consideration of their notional effectiveness.

I have assessed this methodology in advance of its implementation. My conclusion is that the proposed process is capable of undertaking the necessary HFE identification and consideration of error defences required for the GDA phase of the work. The process is very dependent on the quality of the workshops and the composition for them. The methodology does provide minimum requirements and role descriptions that appear appropriate and capable of ensuring the process is well executed.

Dropped Loads HF Analyses – ONR Assessment

Document Title:	**Identification of Dropped loads and Fuel Handling Human Based Safety Claims - Refuelling Machine**	
Document No:	AREVA Report PEPS-F DC 135 Rev. B, July 2012 TRIM Ref. 2012/265588	
PSA nomenclature:	n/a	HEP: n/a
Claim/error description:	Two Fuel Assembly (FA) handling sequences were selected (unloading and loading the core – between core and Fuel Transfer Facility (FTF). One potential direct (i.e. causing an initiating event) HBSC was identified which was an inappropriate action that leads to disengagement of the FA gripper. The potential individual errors that might result in this were analysed to be a selection error (selecting an incorrect control input) or a timing error (disengaging gripper too early). A number of sub-functions and components with critical failure modes that may be susceptible to indirect human causes (i.e. latent errors) are also identified.	

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Risk Importance:	The analysis has considered HFEs related to potential faults on a severity scale defined by EDF and AREVA. In this instance the most onerous event considered is a drop of an FA onto the reactor cavity floor slab; the most severe consequence of this being damage to the slab and/or the FA with an impact on nuclear safety.
Personnel:	Refuelling Machine (RM) operators and maintenance personnel. However, no details are offered to define particular staffing requirements.
Summary of EDF/AREVA Analysis: – Adequacy of design & error defences	EDF and AREVA's approach has sought to identify the potential "Levels of Defence" that will prevent or mitigate the identified human failures in order to judge their adequacy. It is their conclusion that with regard to the dropping of an FA means exist to prevent this occurrence, these include both engineered and administrative aspects and the combination of both should prevent the dropped load from occurring. However, it is noted that the current design is incomplete and whilst it is reasonable to assume and recommend engineered aspects such as prevention of gripper release during transit these aspects will require confirmation and further assessment as design progresses during the site specific phase. For indirect causes the situation is similar with both administrative and engineered measures claimed to be likely to offer protection against such errors but further analysis and confirmation during detailed design will be required.
HFIR items – number & nature	None recorded
Summary of ONR Assessment: – Implementation of methodology – Adequacy of EDF/AREVA consideration of errors & defences:	The methodology specified has been applied successfully and has usefully identified potential HFEs that may result in significant consequences. The extent of the available design and the design stage has prevented further progression of the methodology. At this stage the analysis cannot be considered to have substantiated the identified HBSCs as it has not progressed beyond identification. This is recognised by EDF and AREVA, however the progress afforded by the current design has enabled the clear identification of potential errors and the means by which these may be prevented or mitigated. However, the analysis offered is heavily reliant on assumptions and it is these which must be addressed as design development continues.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Adequacy of existing design:	The current extent of the design has made it impossible to complete the intended analysis in the area of dropped loads. This is recognised within the analysis presented for GDA and the latter stages of the specified methodology will address this. To this end the analysis incorporates extensive assumptions on the design of the equipment to be used and the means by which it will be operated and maintained. The design intent and associated assumptions recorded should provide protection against the identified potential errors but this cannot be confirmed until further design development is undertaken.
Key issues noted:	While the analysis currently only provides identification of potential errors and does not substantiate HBSCs it remains extensively reliant on assumptions with regard to both engineered and administrative aspects of the design and its operation / maintenance.
Key issues for further consideration:	As the analysis progresses to the latter (already specified stages) it will be of particular importance to ensure the resolution of the identified assumptions.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Document Title:	**Identification of Dropped loads and Fuel Handling Human Based Safety Claims – Polar Crane**	
Document No:	AREVA Report PEPS-F DC 134 Rev. B, June 2012 TRIM Ref. 2012/259642	
PSA nomenclature:	n/a	HEP: n/a
Claim/error description:	Two handling sequences were selected that use the Polar Crane. These both relate to the removal and movement of reactor cover slabs and their transition either above the reactor cavity pool or the Reactor Pressure Vessel (RPV). Eleven potential direct (i.e. causing an initiating event) HBSCs were identified that may lead to the dropping of the slab, either immediately or due to a secondary aspect such as a collision or jam. The potential operator driven causes for these are typically incorrect control inputs or a failure to perform checking activities prior to moves. A number of sub-functions and components with critical failure modes that may be susceptible to indirect human causes (i.e. latent errors) are also identified.	
Risk Importance:	The analysis has considered HFEs related to potential faults on a severity scale defined by EDF and AREVA. In this instance the most onerous event considered is a drop of a reactor cover slab; the most severe consequence of this being damage to the RPV head with an impact on nuclear safety.	
Personnel:	Polar Crane operators, including lifting supervisor and maintenance personnel. However, no details are offered to define particular staffing requirements.	

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Summary of EDF/AREVA Analysis: – Adequacy of design & error defences	EDF and AREVA's approach has sought to identify the potential "Levels of Defence" that will prevent or mitigate the identified human failures in order to judge their adequacy. It is their conclusion that with regard to the dropping of a cover slab means exist to prevent this occurrence, these include both engineered and administrative aspects and the combination of both should prevent the dropped load from occurring. However, it is noted that the current design is incomplete and whilst it is reasonable to assume and recommend both administrative and engineered aspects these will require confirmation and further assessment as design progresses during the site specific phase. For indirect causes the situation is similar with both administrative and engineered measures claimed to be likely to offer protection against such errors but further analysis and confirmation during detailed design will be required.
HFIR items – number & nature	None recorded, however a number of definite recommendations are noted, primarily with regard to administrative controls during the lifting tasks.
Summary of ONR Assessment: – Implementation of methodology – Adequacy of EDF/AREVA consideration of claim:	The methodology specified has been applied successfully and has usefully identified potential HFEs that may result in significant consequences. The extent of the available design and the design stage has prevented further progression of the methodology. At this stage the analysis cannot be considered to have substantiated the identified HBSCs as it has not progressed beyond identification. This is recognised by EDF and AREVA, however the progress afforded by the current design has enabled the clear identification of potential errors and the means by which these may be prevented or mitigated. However, the analysis offered is heavily reliant on assumptions and it is these which must be addressed as design development continues.
Adequacy of existing design:	The current extent of the design has made it impossible to complete the intended analysis in the area of dropped loads. This is recognised within the analysis presented for GDA and the latter stages of the specified methodology will address this. To this end the analysis incorporates extensive assumptions on the design of the equipment to be used and the means by which it will be operated and maintained. The design intent and associated assumptions recorded should provide protection against the identified potential errors but this cannot be confirmed until further design development is undertaken.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Key issues noted:	While the analysis currently only provides identification of potential errors and does not substantiate HBSCs it remains extensively reliant on assumptions with regard to both engineered and administrative aspects of the design and its operation / maintenance.
Key issues for further consideration:	As the analysis progresses to the latter (already specified stages) it will be of particular importance to ensure the resolution of the identified assumptions.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Internal Hazards – Internal Flooding GI-UKEPR-IH-03

Document Title:	**EDF/AREVA GDA Human Factors: Internal Flooding**	
Document No:	AMEC Report 16895-707-000-RPT-0013, E-BPE, September 2012 TRIM Ref. 2012/364866	
PSA nomenclature:	n/a	HEP: n/a

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Claim description:	The report covers several claims for manual leak isolation actions for the following: ▪ HR3 - A DN 50 pipe break in the JPI system located in HRB ▪ HR4 - A DN 50 pipe break in the SED system located in HRB ▪ HK1 - A DN 50 pipe break in the JPI system located in HK ▪ HL2 - A DN 50 pipe break in the SEP system located in SAB2 ▪ HD1 - A DN 50 pipe break in the JPV system located in HDA SBO These claims stem from scenarios that assume that a single primary isolation valve has failed. It also includes assessments for key scenarios identified in the final Internal Flooding case (ECEIG12115A submitted with letter ND(NII) EPR01260R) for larger pipe breaks: ▪ For HRB2 (a DEGB (DN 150) in PTR Suction line in HRB) ▪ For HL2 – A DEGB (DN 700) in SEC The assessment spans normal MCR actions in response to alarms (sump alarms) following a wide range of leak scenarios in differing buildings: ▪ Reactor Building (HR A and HR B) ▪ Fuel Building (HK) ▪ Safeguard Buildings (SAB) (HL1 to HL4) ▪ Diesel Buildings (HD) ▪ Nuclear Auxiliary Building (NAB) Most of these scenarios then require local to plant actions to isolate the leaks. The main confounder is where isolation of the fire fighting distribution system (JPI/JPV) is required to isolate a leak. This requires operators to confirm that there is no potential fire and demand on the system prior to undertaking the isolation.[15]

[15] Since the HF submission was submitted a design change has been incorporated that affects the HRB scenarios. Automatic isolation of the sprinkler system occurs after 20 minutes.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Timescales:	HR3/JPI – 1 hour; assessed time = 2hrs 56mins[16] HR4/SED – 1hr 10mins; assessed time = 2hrs 25mins HK1/JPI – 10 hours; assessed time = 3hrs 19mins HL2/SEP – 18-21 hours; assessed time = 4hrs 16mins HD1/JPV – 4-5 hours; assessed time = 2hrs 23mins HRB2 (DN 150) – 41mins; assessed time = 41mins HL2 (DN 700) – 35mins; assessed time = 31mins
Risk Importance:	These isolations are judged as being equivalent to high risk – due to their importance to the deterministic safety case requirements.
Personnel:	All the base cases for these isolations required MCR actions for leak detection & most leak source identification – performed by OA, OS & supported by the SS/SE. FOs undertake LTP actions to close the necessary valves in the relevant buildings.
Summary of EDF/AREVA Analysis: – Adequacy of substantiation	EDF and AREVA have undertaken a detailed TA including detailed timeline assessment for FO journey times to isolation locations. This uses a 1kmhr^{-1} speed on a CAD plant model to allow for access & journey elements (doors, stairs, steps etc.). The analyses assume that flooding occurs during normal operation and entry into SOA operation is not required. The analyses generally show: – Leak detection is apparent for all leaks via high sump alarms – Leak site determination is generally more difficult due the lack of clear indication of the leak site; consequently detailed leak response procedures are needed to undertake systematic leak site determination The operators will have to check that the fire fighting system is not required before isolating the JPI system

[16] The time available for successful operation for the HR3 and HR4 scenarios has increased since the HF analyses were completed due to design changes that have relaxed the demands on operator actions.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

HFIR items – number & nature	HFIR items 094-118. These cover several general issues: – The procedures need to contain sufficient detailed information for reliable leak detection and response (particularly for systematic leak source identification) – The HMI lacks specific parameter information to aid the MCR operators in leak response – The response times for situations with concurrent faults (leading to SOA entry) need to be considered for acceptability – For the HR3 & HR4 scenarios motorised valves need to be installed to remove the need for local to plant actions – The operators determine that there is no fire risk (for JPI isolations) by referring to a dedicated fire alarm panel. If alternative fire risk surveillance methods (e.g. location CCTV) then this may increase the leak isolation times HFIR 178 (added following ONR comments) on ensuring the LTP isolation procedure specifies the optimum task sequence. HFIR 179 – this recommends consideration of automation of some leak isolation tasks for HRB2c. HFIR 180 – this identifies the need to include manual stopping of the SEC pumps as the primary means of leak isolation for the HL2 scenario.

Annex 5

Assessment Summary for Dropped Loads and Internal Flooding

Summary of ONR Assessment: – Adequacy of EDF/AREVA consideration of claim:	The analysis has been detailed and identified all key PSFs influencing task performance and reliability. Particular attention has been made on FO actions and the journey times; and on the challenges of leak detection & leak source identification. The HFIR items encompass most key issues that appear relevant to supporting these isolation claims. The main issue that does not appear to have been addressed is confirmation that the internal flooding scenarios do not lead to the generation of other alarms. If other alarms are generated this could mask the relevant leak alarms or lead to delays in response due to the operators having to deal with a more complex situation. The report indicates that this needs to be addressed further post-GDA. ONR agrees with the need for automation of valve closure for the HR3 & HR4 scenarios. The detailed HMI and procedural issues identified by the analyses need to be implemented to adequately support all the other claims.
Degree of substantiation:	Not at all for HR3 & HR4 – unless the recommended design modification is adopted (then fully substantiated for full automation) Partially – for the other scenarios.
Key issues noted:	As HFIR items and consideration of the potential for additional alarms to be generated.
Key issues for further consideration:	As issues noted.[17]

[17] Several design changes have been made since the completion of the HF analyses and ONR's HF assessment. This has included the recommended design modifications identified in the HFIR items; and automatic isolation of the JPI system in the HRB building after 20 minutes.