Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Human Factors Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-028
Revision 0
11 November 2011

COPYRIGHT

First published December 2011

For published documents, the electronic copy on the ONR website remains the most current publically available version and copying or printing renders this document uncontrolled.

PREFACE

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

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

EXECUTIVE SUMMARY

This report presents the findings of the Human Factors assessment of the UK EPR reactor undertaken as part of Step 4 of the Health and Safety Executive's Generic Design Assessment. My assessment has been carried out on the Pre-Construction Safety Report (November 2009) and supporting documentation submitted by EDF and AREVA during Step 4.

My assessment has followed a step-wise approach in a claims-argument-evidence hierarchy, corresponding to Generic Design Assessment Steps 2, 3 and 4 respectively. In the technical area of human factors, no assessment was undertaken in Generic Design Assessment Step 2, and my Generic Design Assessment Step 3 Assessment Report was more aligned to a Generic Design Assessment Step 2 Assessment Report; focusing on consideration of EDF and AREVA's claims, with very limited consideration of the available arguments. As a result my assessment has been back-loaded to Generic Design Assessment Step 4, during which I have examined in detail the arguments and supporting evidence for the human based safety claims.

It is seldom possible or necessary to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is undertaken in a focused, targeted and structured manner with a view to revealing any topic specific or generic weaknesses in the safety case. To identify the sampling for the human factors area an assessment plan for Generic Design Assessment Step 4 was developed in advance.

The following items have been agreed with EDF and AREVA as being outside the scope of Generic Design Assessment (Phase 1) for human factors:

- Team organisation.
- Staffing.
- Operating and maintenance procedures.
- Use of State Orientated Approach.
- Display breakdown.
- Training.

It has been necessary for EDF and AREVA to make assumptions with regard to these aspects in the Generic Design Assessment risk assessment, but finalisation of them will not occur until Generic Design Assessment Phase 2 (site licensing); where they will largely be the responsibility of a prospective licensee organisation. However several notable elements have been embedded within the substantiation of human based safety claims for Generic Design Assessment Phase 1, hence any future licensee wishing to adopt alternative approaches would be required to justify the changes. These elements are:

- The application of the State Orientated Approach and procedures for abnormal operations.
- The main control room staffing philosophy comprising a strategy operator, action operator and supervisor/safety engineer.

My assessment has focussed on five key work streams that address the breadth of human factors within a Pre-Construction Safety Report. These are:

1 Substantiation of Human Based Safety Actions

This work stream focused on ensuring that the risks from human actions have been reduced to As Low As Reasonably Practicable. It is the foundation for my risk informed

assessment and supports the Generic Design Assessment, assessment strategy of considering the claims, arguments and evidence. The overriding aim of this area of assessment is to ensure the adequacy of the substantiation[1] of important operator actions. Subsidiary to this, the work stream aimed to provide a judgement on the:

- Completeness of the statement of 'claims on the operator'.
- Adequacy of the justification, or process intended to ensure, that claims are reasonable and will be achievable by the realised design.
- Recommendations on any key area of follow-on work and assessment that is required to ensure that key claims are substantiated.

By addressing these aims, my assessment intended to judge whether all key areas of reliance on operator actions or vulnerability to human errors have been identified and sufficiently considered for this stage in the overall development of the design and its assessment.

2 Generic Human Reliability Assessment

Work Stream 2 aimed to look generically at particular aspects of the Human Reliability Assessment across the safety submission; and particularly the Human Reliability Assessment methods and their application adopted by EDF and AREVA. Further to this I assessed the general suitability of the techniques applied in light of the digital nature of plant and equipment control systems and interfaces.

3 Engineering Systems

This work stream principally sought to address the maintainability and maintenance reliability of the UK EPR from a human factors perspective. The work stream was important to ensure that the claims and assumptions regarding the reliability of systems and components were adequately underpinned by the evidence produced.

4 Human Factors Integration

Work Stream 4 focussed on the general processes and mechanisms in place to deliver quality human factors input to the design of the UK EPR and its safety case for the UK. This work stream was particularly important given ND's sampling and targeted approach to assessment. As this approach does not assess the entirety of a safety submission, this element of the assessment sought to provide me with a level of confidence that the human factors analyses and design input not assessed during the Generic Design Assessment are of suitable quality to inform the design and safety submission, and ultimately to support reliable human intervention.

5 Plant-wide generic Human Factors assessment

This work stream complements Work Stream 1 and assesses generic human factors issues that would not necessarily be highlighted as part of Work Stream 1. Whereas Work Stream

[1] Substantiation is a composite of the veracity of the underlying evidence and a judgement regarding the validity or proof of an assertion, statement or claim.

1 considers the depth of human factors analyses, Work Stream 5 aims to assess across the breadth of human factors analyses in order to provide a judgement on the adequacy of the overall plant design, and how well it meets modern standards and adopts recognised good practice. It is an important area to ensure that the design meets As Low As Reasonably Practicable requirements.

The main conclusions of my assessment in each area are:

Substantiation of Human Based Safety Claims

Overall I judge that EDF and AREVA have not provided an adequate substantiation of the human based safety claims at the end of Generic Design Assessment Step 4. The main deficiencies are:

- The incompleteness of the identification of human based safety actions; particularly for pre-fault (Type A) activities.
- Inadequate detailed task analysis to support the significant human based safety claims (these are primarily post-fault operator actions). Only four human based safety claims have been analysed.

This gap was highlighted in my Generic Design Assessment Step 3 assessment conclusions, and identified early on in my Generic Design Assessment Step 4 assessment process.

The lack of substantiation I judge to be significant, and has the additional consequence that I consider that EDF and AREVA are not in a position to meet As Low As Reasonably Practicable requirements from a human factors perspective. As a result, I propose a Generic Design Assessment Issue (**GI-UKEPR-HF-01** refers) to address both the incompleteness of the identification of human based safety claims, and provision of proportionate supporting evidence to support those claims. This also captures my regulatory observations in the areas of pre-fault actions, misdiagnosis, violation potential, and post-fault action substantiation. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

I have collaborated with Probabilistic Safety Analysis colleagues and I judge that the Human Reliability Assessment and Probabilistic Safety Analysis model does provide an acceptable basis for determining the overall risk contribution from human actions at a Pre-Construction Safety Report stage. I have identified areas where more evidence is required to justify the Human Reliability Assessment claims and these are cited as Assessment Findings, to be addressed as routine business as the safety case for the UK EPR progresses beyond the design stage. I have aligned these findings with the expectation from my Probabilistic Safety Assessment colleagues that the Human Reliability Assessment will be updated post the Pre-Construction Safety Report phase.

Generic Human Reliability Assessment

The current UK EPR Human Reliability Assessment is essentially an ‘assumptions based’ analysis that lacks adequate substantiation from appropriate task analysis of pre and post-fault operator actions. However my examination of the Human Reliability Assessment for both Level 1 and 2 Probabilistic Safety Analysis indicates that an acceptable consideration of the contribution from operator error to the overall risk has been made at this point.

The Human Reliability Assessment method applied to the Level 1 Probabilistic Safety Analysis Human Reliability Assessment is generally satisfactory, although a greater consideration and inclusion of pre-fault human actions (both Type A and B) will be required in the proposed Human

Reliability Assessment revision, as will an improved consideration of human error dependency. The consideration of human failure initiating events, particularly for low power and shutdown states appears to be incomplete, and this could be significant for these plant states. I will take these observations forward as Assessment Findings; to be addressed in line with the update of the Probabilistic Safety Assessment.

Engineering Systems

EDF and AREVA have undertaken work related to maintenance, which has the potential to support human reliability, and there is some evidence of the application of operational experience and design input to support their claims in this area. However there appears to have been strong reliance on the implementation of human factors by designers and contractors without adequate human factors specialist support. In recognition of the uncertainty I have over the adequacy of EDF and AREVA's approach, I propose to take my assessment observations forward in two ways; via Generic Design Assessment Issue Action **GI-UKEPR-HF-01.A2**; relating to the consideration of pre-fault human actions, and via Assessment Findings relating to the detailed design and verification requirements for the UK EPR equipment.

Human Factors Integration

In general I judge that EDF and AREVA have evidence of aspects of a Human Factors Engineering programme of work; but not of an overall Human Factors Integration plan that meets my expectations. What has been provided is 'piecemeal' and is focused on the Main Control Room design. There has been an over-reliance on the use of operational experience, rather than formal safety analysis, and on design guidance provided to engineers. This does not provide me with confidence that the risk from human error has been reduced to As Low As Reasonably Practicable. However as Human Factors Integration is process based, this will be taken forward via an Assessment Finding; to be addressed by a prospective licensee.

Plant-wide Generic Human Factors Assessment

I consider that in general the quality of the design based human factors aspects across the wide range of areas assessed (Allocation of function; Workplace and workstation design; Working environment; Control and display interfaces; Procedures; and Staffing and work organisation) appear to be adequate and will not significantly undermine human reliability. The Main Control Room design supports the design basis operating organisation (Flamanville 3) and the use of State Orientated Approach procedures well. I note many minor observations across the assessment area and these are cited as Assessment Findings to be addressed post Pre-Construction Safety Report. However due to the limited evidence provided in Generic Design Assessment Step 4, there will be a requirement for a future licensee to undertake detailed studies to confirm the adequacy of the design, particularly for non-Main Control Room locations.

Overall Conclusions

EDF and AREVA have not presented an adequate safety case for human factors for the UK EPR, and the position has not moved on significantly from the end of Generic Design Assessment Step 3. EDF and AREVA have provided some additional evidence relating to their design process, but much of this was received late in my assessment. They have only been able to provide a very small part of the required substantiation for their key human based safety claims. This results in a substantial gap in their safety submission for Generic Design Assessment remaining at the end of

Generic Design Assessment Step 4. I accept that there is a significant difference in the regulatory approach to human factors between the United Kingdom and France, and I consider that this has contributed to the position. In consequence I have raised Generic Design Assessment Issue **GI-UKEPR-HF-01** to reflect the significant gap in the safety submission that remains at the end of Generic Design Assessment Step 4.

The material that I have assessed to form my judgements has largely been extracted from the considerable amount of documentation provided from the Flamanville 3 design. EDF and AREVA have not provided a consolidated human factors safety case based on appropriate human factors analyses aligned with United Kingdom expectations. For the UK EPR, the only targeted human factors analysis offered has been the qualitative substantiation of four human based safety claims. This is inadequate for a Pre-Construction Safety Report. Furthermore, the timing of documentation supplied, predominantly in response to regulatory questions and observations, was delivered very late in the Generic Design Assessment Step 4 process, and I have not been able to assess it in its entirety.

However, I do not object to progression of the UK EPR design on human factors grounds principally due to the fact that it is an evolution of a standard Pressurised Water Reactor; which benefits from significant operating experience (particularly relating to N4 and Konvoi plants), and detailed fault studies. The EPR Probabilistic Safety Analysis model shows that the importance of human error to public and worker risk is limited. Furthermore, should subsequent human factors assessment reveal further deficiencies in the design or safety analysis, human factors solutions can typically be developed and implemented without undue effect on the design of major civil or pressure system components or their layout. On this basis it is unusual for gross disproportionate arguments to be made relating to human factors solutions. I therefore consider that progression post Pre-Construction Safety Report will not result in the foreclosing of options associated with human factors.

LIST OF ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
AD	Automatic Diagnosis
AF	Assessment Finding
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
ANS	American Nuclear Society
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ASN	Autorité de Sûreté Nucléaire (French Nuclear Safety Authority)
ATHEANA	A Technique for Human Event Analysis
BMS	Business Management System
BS	British Standards
C&I	Control and Instrumentation
CAD	Computer Aided Design
CAHR	Connectionist Assessment of Human Reliability
CBDT	Cognitive Based Decision Tree
CCWS	Component Cooling Water System
CDF	Core Damage Frequency
CESA	Cognitive Error Search and Assessment
CHRS	Containment Heat Removal System
CNEN	Centre National d’Etudes Nucléaire
COL	Combined Operating Licence
COTS	Commercial Off The Shelf
CREAM	Cognitive Reliability and Error Analysis Method
DAC	Design Acceptance Confirmation
DG	Diesel Generators
DRI	Installation Rules Datasheets
EBS	Extra Boration System
EDF	Electricité de France
EDG	Emergency Diesel Generators Page 104
EFWS	Emergency Feed Water System
EOP	Emergency Operating Procedures
EPR	European Pressurised Reactor
EPRI	Electric Power Research Institute
EPRI-HRA	Electrical Power Research Institute Human Reliability Analysis Calculator
FAP	Forward Action Plan

LIST OF ABBREVIATIONS

FA3	Flamanville 3
FLIM	Failure Likelihood Index Methodology
FO	Field Operators
FSCD	Fast Secondary Cooldown
FSER	Final Safety Evaluation Report
FV	Fussell-Vesely
GDA	Generic Design Assessment
HAZOP	Hazard and Operability (Study)
HCI	Human Computer Interaction
HCR	Human Cognitive Reliability
HCR	Human Cognitive Reliability
HEART	Human Error Assessment and Reduction Technique
HED	Human Error Dependence
HEI	Human Error Identification
HEP	Human Error Probability
HF	Human Factors
HFE	Human Factors Engineering
HFE	*Human Failure Event*
HFI	Human Factors Integration
HFIP	Human Factors Integration Plan
HFIR	Human Factors Issues Register
HFPFMEA	Human Factors Process Failure Modes and Effects Analysis
HMI	Human Machine Interface
HPLV	Human Performance Limiting Value
HRA	Human Reliability Assessment
HSE	Health and Safety Executive
HTA	Hierarchical Task Analysis
IAEA	International Atomic Energy Agency
IDAC	Information, Decision and Action in Crew
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IRWST	In-containment Refuelling Water Storage Tank
ISA	Instantaneous Self Assessment
ISO	International Standards Organisation
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accident

LIST OF ABBREVIATIONS

LOCC	Loss Of Cooling Chain
LOFW	Loss Of Feed Water
LOOP	Loss of Offsite Power
LRF	Large Release Frequency
MCR	Main Control Room
MDEP	Multi-National Design Evaluation Programme
MFWS	Main Feedwater System
MHSI	Medium Head Safety Injection
NARA	Nuclear Action Reliability Assessment
NASA	(United States) National Aeronautics and Space Administration
ND	Nuclear Directorate
NF	French Norms
NPP	Nuclear Power Plant
OA	Operator Action
OECD	Organisation for Economic Co-operation and Development
OEF	Operating Experience Feedback
ORE	Operator Reliability Experiments method
OL3	Olkiluoto 3
ONR	Office for Nuclear Regulation
ORE	Operator Reliability Experiments
OS	Operator Strategy
OSSA	Operating Strategy for Severe Accidents
PCSR	Pre-Construction Safety Report
PCmSR	Pre-Commissioning Safety Report
PICS	Process Information and Control System
POP	Plant Overview Panel
PORV	Pressure Operated Relief Valve
PPE	Personal Protective Equipment
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
PSF	Performance Shaping Factors
PWR	Pressurised Water Reactor
QA	Quality Assurance
RHR	Residual Heat Removal
RIF	Risk Increase Factor
RO	Regulatory Observation

LIST OF ABBREVIATIONS

ROA	Regulatory Observation Action
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown Station
SAP	Safety Assessment Principle
SBO	Station Black Out
SE	Safety Engineer
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SHARP1	Revised Systematic Human Action Reliability Procedure
SICS	Safety Information and Control System
SI	Safety Injection
SLIM-MAUD	Success Likelihood Index Methodology – Multi Attribute Utility Decomposition
SOA	State Orientated Approach
SPAR-H	Standardised Plant Analysis Risk – Human Reliability Analysis
SQEP	Suitably Qualified and Experienced Person
SS	Supervisor
SSS	Start-up and Shutdown Feedwater System
STUK	Säteilyturvakeskus (Finnish Radiation and Nuclear Safety Authority)
SZB	Sizewell B
TA	Task Analysis
TAG	Technical Assessment Guide
THERP	Technique for Human Error Rate Prediction
TQ	Technical Query
TRC	Time Reliability Correlation
TSC	Technical Support Centre
TSC	Technical Support Contractor
TTA	Tabular Task Analysis
UK	United Kingdom
UMH	University of Maryland Hybrid
US	United States
USA	United States of America
US NRC	United States Nuclear Regulatory Commission
V-LOCA	Interfacing system loss of coolant accident
VDU	Visual Display Unit
WENRA	Western European Nuclear Regulators’ Association

TABLE OF CONTENTS

Tables

Figures

Annexes

1 INTRODUCTION

1 My report presents the findings of the Human Factors (HF) assessment of the United Kingdom (UK) European Pressurised Reactor (EPR) safety submissions made by Electricité de France (EDF) and AREVA under the Health and Safety Executive (HSE) Generic Design Assessment (GDA) process. I assessed the Pre-construction Safety Report (PCSR) November 2009 (Ref. 17) and its supporting evidentiary information derived from the Master Submission List (Ref. 18). My assessment has been undertaken in line with the requirements of the Business Management System (BMS) document (Ref. 2) T/AST/001 which sets down the process of assessment within the Nuclear Directorate and explains the process associated with sampling of safety case documentation. I used the Safety Assessment Principles (SAP) (Ref. 4) as the basis for my assessment, together with relevant Technical Assessment Guides (TAG), which underpins the SAP. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 In accordance with the HSE guidance document (Ref. 5) my work on GDA has been conducted in a step-wise approach with the assessment becoming increasingly detailed at each step.

GDA Step 1 The preparatory part of the design assessment process involving discussions between the Requesting Party and the Regulators (HSE ND) to agree requirements and how the process would be applied.

GDA Step 2 An overview of the fundamental acceptability of the proposed reactor design concept within the UK regulatory regime to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being licensed in the UK.

GDA Step 3 An ND review of the safety aspects of the proposed reactor design to progress from the fundamentals of Step 2 to an analysis of the design, primarily by examination at the system level and by analysis of the RP’s supporting arguments.

3 However, in the area of HF, no work was undertaken in GDA Step 2 and my assessment in GDA Step 3 was limited to examination of the human based safety claims, with some consideration of the supporting arguments, due to my late start part way through the GDA Step 3 process. As a result, the HF assessment has been back-loaded to GDA Step 4 where I have undertaken the majority of my GDA assessment.

4 This is the report of my work in GDA Step 4, which was an in-depth assessment of the PCSR [the ‘safety case’] and relevant supporting documentation. For HF this included a detailed examination of the arguments and evidence, on a sampling basis, provided by the safety analysis presented in the GDA submissions.

5 Completion of GDA Step 4 represents the end of my planned GDA assessment on the topic of HF for the EDF and AREVA UK EPR.

2 EDF AND AREVA'S SAFETY CASE

2.1 Introduction

6 At the end of GDA Step 3, I concluded that the EDF and AREVA PCSR November 2009 had not presented an adequate case for HF for the UK EPR; stating "*there is no recognisable UK structure to the documentation for assessment (i.e. claims, arguments and evidence approach) and there is very limited and often no analysis or arguments presented in the PCSR chapters that I have considered."* This resulted in me raising RO-UKEPR-38 requiring that: *"The Requesting Party …submit(s) documentation that clearly defines the role of human actions on the UK EPR (i.e. the safety 'claims') and justifies those actions via human factors analysis (i.e. the 'arguments' and 'evidence')*."

7 EDF and AREVA proposed a Response Plan (Ref. 89), which I subsequently advised was not adequate against the requirements of RO-UKEPR-038. Through regulatory exchange, it became apparent that there was not an extant HF safety case available for Flamanville 3 (FA3) that could be cited for UK EPR, or indeed formal HF analyses of the type typically expected to underpin UK safety cases. EDF and AREVA advised that this was essentially due to the difference in approach to HF between France and the UK. In addition, EDF and AREVA advised that analyses of the type expected by UK regulators would have to be developed specifically for the UK. I therefore requested that EDF and AREVA investigate what existing human factors analysis was available (e.g. to support FA3) that could be submitted in support of the GDA for the UK EPR. In response EDF and AREVA updated their Plan and proposed a 'Forward Action Plan' (FAP) of qualitative HF analyses of the type I expect (Ref. 44 dated 30 April 2010). However as this was now ~5 months into GDA Step 4, available time and resource was cited by EDF and AREVA as a factor in determining what could now reasonably be achieved to support their GDA Step 4 submission for HF. This FAP proposed development and submission of four detailed task analyses and an associated method statement, and the production of two Human Reliability Assessment (HRA) handbooks within GDA Step 4. There was also additional documentation submitted in response to specific Technical Queries (TQ) and Regulatory Observations (RO) raised throughout GDA Step 4.

8 EDF and AREVA have not presented a consolidated human factors safety case for the UK EPR that matches ND's expectations for the PCSR stage of the design; and as a result RO-UKEPR-038 was not closed during my assessment process.

9 HF information and related safety arguments are contained in the following principal references that were available at the start of GDA Step 4; and it is these that have primarily formed the basis of my assessment:

- UK EPR PCSR November 2009 Chapter 18.1: Human Machine Interface.
- UK EPR PCSR November 2009 Chapter 15: Probabilistic Safety Analysis.
- UK EPR PCSR November 2009 Chapter 7 Appendix 7a: Detailed Description of the C&I Systems….General Description of Nuclear island I&C.
- NEPS-F DC 191 Human Reliability Handbook of the UK EPR PSA Level 1.
- NEPS—F/10.273 Identification and Substantiation of the Key Claims on Operator Reliability in the UK EPR PSA Level 1.
- 30 NEPS-F DC 527 Revision A UK EPR Level 2 Supporting Human Reliability Analysis. AREVA.

- ECEF012001A. EDF. (E) Approach for integration of human factors in EPR design.
- Task analyses to support 4 human based safety claims. (Refs 40, 41, 42 and 43).

10 EDF and AREVA also submitted an updated PCSR Chapter 18.1 in March 2011. However, as this was a significant re-write of the earlier PCSR, I will assess this post GDA Step 4.

2.2 Quantitative HRA

11 The probabilistic claims on human actions are presented in the Level 1 and Level 2 HRA Handbooks (Refs 29 and 30). These reflect the 2009 PSA model which has been updated in 2011. This update, along with any human reliability assessment (HRA) revisions, has not been included in my assessment.

12 For the assessed Level 1 Probabilistic Safety Analysis (PSA) there are 189 Type A human failure events (*HFE*) (pre-initiating fault *HFEs*), limited to mal-operation of manual valves; 9 Type B *HFEs* (*HFEs* leading to an initiating event); and 59 Type C HFEs.

13 EDF and AREVA state that potential errors in the maintenance of components are not included in the systems analysis, as such errors are judged to have been counted in the failure rate estimates for components (Ref. 34). Multiple maintenance errors have been discounted as EDF and AREVA judge that post-maintenance tests would directly recover such errors. Hidden multiple maintenance errors that are not directly recovered are considered by them to be part of the contribution to common cause failures.

14 The HRA numerical assessment for the Level 1 PSA Type C *HFEs* applies the Accident Sequence Evaluation Program (ASEP). A summary of the assessment of post-fault *HFEs* is provided, with basic details of the basis for the HRA quantification (e.g. time available, cues to the operator, task location, stress level, risk importance, dependency). These post-fault operator actions fall into several main groups:

- Bleed (or Feed and Bleed).
- Isolation of dilution.
- Partial cooldown, fast cooldown and secondary heat removal.
- Make up with LHSI (shutdown states).
- Residual heat removal with LHSI in shutdown states.
- In-containment Refuelling Water Storage Tank (IRWST) cooling.
- Trip of reactor coolant pumps.
- Start-up of SBO diesels.
- Operator actions following SGTR.
- Isolation of V-LOCA.
- Fuel Pool Accident.
- Miscellaneous.

15 The most important post fault operator actions (actions with a Fussell Vesely (FV)>1% and Risk Increase Factor (RIF)>2) are presented in Table 1 (based on PCSR November 2009 Chapter 15.7):

Table 1: Level 1 PSA Most Important Operator Actions

Failure Description	Nominal Probability per Demand	FV	RIF
Operator fails to initiate Fast Cooldown in 30 minutes	$4.3\text{x}10^{-2}$	12.8%	3.9
Operator fails to initiate Feed and Bleed in 120 minutes	$8.1\text{x}10^{-3}$	9.1%	9.0
Operator fails to start LHSI in the event of Loss Of Cooling Chain (LOCC) in 120 minutes	$2.1\text{x}10^{-3}$	6.8%	32.6
Operator fails to cross-connect the Emergency Feedwater System (EFWS) tanks / Operator fails to re-feed Start-up and Shutdown System (SSS), Main Feedwater System (MFWS) or EFWS tank	$1.0\text{x}10^{-4}$	3.5%	350.3
Operator fails to start Station Black Out (SBO) diesels or to close breakers within 2 hours	$2.2\text{x}10^{-3}$	3.2%	12.1
Operator fails to start and control EFWS in case of Protection System (PS) failure within 1 hour	$2.8\text{x}10^{-3}$	2.9	14.6

16 The most important operator action modelled in the Level 1 PSA (based on the RIF value) is the manual opening of the EFWS header before 6 hours. If the secondary RHR is provided by the steam generator safety valves (MSSV), the operator has to initiate the make up of the MFWS tank or to cross connect the EFWS tanks before 6 hours have elapsed. The assumed failure probability is $1.0\text{x}10^{-4}$. EDF and AREVA carried out a sensitivity study to assess the importance of this action, by multiplying the failure probability by 10. The result reveals that the core damage frequency (CDF) is sensitive to this (+32%). However EDF and AREVA assert that the current failure probability of $1.0\text{x}10^{-4}$ *"is a reasonable value considering the time available to perform the action, the crisis team intervention and the controlled state of the plant (no break)."*

17 Further sensitivity studies were carried out relating to manual actuation of feed and bleed; CDF not sensitive to a less conservative time availability and dependency between operator actions. This latter study revealed that the overall CDF result is sensitive to the dependency modelling and it is highlighted that the increase (+18% for high dependencies between operator actions and +41% for total dependency between operator actions) is mainly linked to the dependency between the manual action to initiate secondary partial cooldown before 15 minutes, and the manual action to initiate feed and bleed in the event of small primary break before 30 minutes.

18 I note that operator actions in general contribute 28% to the overall CDF (from Fig 3 in PCSR Ch15.7).

19 I further note that one of the key assumptions in the Level 1 PSA is that *"the Human Reliability Analysis is performed with the assumptions that the operating procedures and guidelines will be well written and complete, as will operator training."* (Ref. 29).

20 The Level 2 PSA includes actions from the Level 1 PSA and a small number of additional actions to mitigate severe accidents. The HRA applies the SPAR-H method, as EDF and AREVA claim that this method has a wider range of performance shaping factors that are

better able to represent the complexity of decision making being modelled in Level 2 scenarios.

21 The most significant operator actions from the Level 2 PSA are presented in Table 2.

Table 2: Level 2 PSA Most Important Operator Actions

Failure Description	% contribution to Large Release Frequency (LRF)
Level 1 operator error to start SBO	12
Level 1 operator error to perform primary fast cooldown	6
Dependent operator failure to enter the OSSA guidelines	7.0
Dependent operator failure to enter the OSSA guidelines in the long term, after failing to enter the OSSA early	6
The following operator actions contribute more than 5% to LRF	
Operator failure to open the RCS depressurisation valves within 40 min	5
Level 1 operator error to perform primary fast cooldown within 30 min	11
Level 1 operator error to perform primary cooldown	7
Level 1 dependent operator error to perform feed and bleed within 30 min	7

22 The 'HRA handbooks' for the Level 1 and Level 2 HRAs (Refs 29 and 30) present the *HFEs* and offer some supporting qualitative information relating to the task. For the Level 1 PSA, this additional qualitative information is a statement of the time available for the task; the stress level (medium/high), the task location and cues to the operator. I note that this information is factual (e.g. statements on the presence of alarms and indications) rather than analysis based argument and evidence to underpin the statements made. For the level 2 PSA, there is a focus on explanation of the quantification approach, which applies an adapted SPAR-H model. There is consideration of Performance Shaping Factors (PSF) in terms of available time and 'cues'. The time requirements are based on engineering judgement - there is no qualification of the quality of the cues; only a statement of their presence. There is also a consideration of dependency modelling. There is detailed information presented on the OSSA approach and description of the expected emergency organisation. There is no qualitative analysis to support the quantifications.

23 There is also specific discrete analysis of potential accident sequences in the fuel pool and specific operator actions to mitigate such accident sequences via: initiating additional trains of fuel pool cooling; initiating longer term make up to the fuel pool and undertaking repair actions in the longer term. Failure of these operator actions are significant contributors to the frequency of occurrence of boiling in the fuel pool and fuel damage frequencies. However I note that the overall risks arising from fuel pool accidents are very low in comparison to those modelled in the main PSA.

24 I note that the deterministic safety case contains one F1A (equivalent to a Class 1 system) action (action required for an event to reach the controlled state) relating to a

steam generator tube rupture (SGTR). All other operator actions are F1B actions; actions required to achieve the safe shutdown state.

2.3 Human Factors Engineering (HFE)

25 Chapter 18.1 of the November 2009 PCSR is the principal reference for the human factors presentation of information. This chapter describes the HF programme for the FA3 design and focuses on the method; content of the HFE programme; implementation for FA3 and the management of the HF team and effort. I note that this chapter is only ~50 pages of material. The material presented is descriptive and largely prospective or hypothetical; what will or can be achieved through the elements of HFE mentioned, and there is often a brief narrative on the importance of programme element. The majority content of the November 2009 PCSR Chapter 18.1 is 'design principles and functions', although the material is very high level and not linked through to referenced evidence. There is citation of 'requirements' although they appear to be high level design goals rather than specific standards to be adhered to.

26 Description is provided of the management of the HFE programme for the (generic) EPR project (i.e. not necessarily what has been applied to the UK EPR project). Of note is that the role of HF specialists is to integrate operating experience from existing plants; provide a HF perspective with regard to design studies and choices; integrate requirements from standards and principles relating to HF that are applicable; and to 'integrate studies evaluating the design choices. Of interest is that there is no mention of responsibility for design, implementation and delivery of a recognisable Human Factors Integration (HFI) programme and very limited mention of a link to the wider risk and safety assessment work (c.1 page).

27 The material is not presented in a claims, arguments, and evidence structure and the format and content is not analogous to a UK safety case. There is no HF analysis presented throughout. There is also no mention of "as low as reasonably practicable" (ALARP) or UK specific requirements.

28 The safety argument for the HF aspects of the EPR appears to be based on empirical observations of phenomena on existing fleet; adoption of positive features and design elements and elimination of less successful features and design elements. EDF and AREVA cite a four stage approach to the HFE programme: analysis of the 'existing situation'; definition of principles relating to the role of operators; incorporation of those principles into functional specifications; and the adjustment of design specifications following HF review. I note that there is no mention of a risk informed or driven approach to the targeting of HFE work.

29 A key safety argument proposed by EDF and AREVA that that the basic safety functions and detailed allocation of function between people and plant has been determined for previous plants (Konvoi and N4) and that the UK EPR is built on this foundation.

30 The state oriented approach (SOA) and computer base procedures were employed on earlier generation French designs, but the automatic diagnosis (AD) feature is novel to the EPR and was developed in response to operating experience. The SOA and the AD system is novel to the UK and somewhat different to the post fault operating philosophy currently adopted in the UK. Therefore I would have expected the PCSR to have provided detail argument and evidence to demonstrate how these features support human reliability; however no evidence is offered in this regard.

31 In addition to Chapter 18.1, EDF and AREVA submitted four detailed task analysis in response to regulatory intervention, for operator start-up of the SBO diesels following loss

of off-site power; operator initiated cooldown; manual pump maintenance and manual EFWS refill. These analyses aim to evaluate the feasibility of operator actions associated with safety case claims by demonstrating the allocation of function decision, identifying areas where operators can negatively influence nuclear safety; providing a qualitative basis for subsequent quantification of human error and to provide an ALARP position. The four analyses appear to be the only substantive qualitative substantiation and recognisable analysis offered by EDF and AREVA in terms of a UK safety case. These represent a very small sample of the volume that I would typically expect for a PCSR submission.

32 Further material was offered relating to operator misdiagnosis and violation potential, and HFI, again in response to regulatory intervention. This material was submitted late in the GDA Step 4 process (December 2010 and January 2011) and although I acknowledge its delivery, I was not able to fully consider the complete content in GDA Step 4 and therefore I have not summarised it here.

3 ONR'S ASSESSMENT STRATEGY FOR HUMAN FACTORS

33 My assessment plan (Ref. 1) identified the scope of the assessment and the standards and criteria that would be applied. This is summarised in Section 3.2 of this report.

3.1 Human Factors in Context

34 HF is the scientific study of human physical and psychological capabilities and limitations and the application of that knowledge to the design of work systems. Within the nuclear context, HF is concerned with the human contribution to nuclear safety during facility design, construction, commissioning, operation, maintenance, and decommissioning. ONR requires that a systematic analytical approach be applied to understanding the factors that affect human performance/reliability within the context, and a demonstration that the potential for human error to adversely affect nuclear safety is reduced to ALARP.

3.1.1 Human Factors in the Pre-Construction Safety Report

35 T/AST/051 provides general ONR guidance on the purpose, scope and content of nuclear safety cases. T/AST/051 (Ref. 7) states that *'for plants under design …the safety case at each stage should contain enough detail to give confidence that the safety intent will be achieved in subsequent stages.'* T/AST/051 (Ref. 7) also describes the particular purpose of PCSR to be to demonstrate that:

- The detailed design proposal will meet the safety objectives prior to commencement of construction or installation.
- The plant is capable of being operated within safe limits.
- Sufficient analysis has been performed to prove that the plant will be safe.
- Outstanding confirmatory work has been identified.
- The risk will be ALARP.
- Decommissioning is feasible.

36 In addition, the general philosophy of the PCSR phase is to ensure that design options are not foreclosed, i.e. that construction is not commenced until it is clearly demonstrated by engineering and scientific analysis that the proposed design is the optimum ALARP solution. For example, if construction were to commence without such assurance, it is reasonably foreseeable that fundamental analysis undertaken during construction may indicate design solutions that were no longer achievable, thereby compromising the ALARP position.

37 Our expectations for the HF contribution to the PCSR stage are illustrated in Figure 1 (taken from T/AST/058 (Ref. 7)) which also includes my analysis expectations for the preliminary safety case phase. Readers are referred to T/AST/058 (Ref. 7) my Technical Assessment Guide (TAG) on HFI which describes my analysis expectations for the pre-commissioning, pre-operational, site wide, periodic safety review and post operational safety cases. Broadly, my expectations are that the majority of HF analysis work should be undertaken for PCSR, such that it can influence the design and input to the risk assessment. As the design progresses, my concerns move towards verification and validation of the human based safety claims and an increased emphasis on training activities and evaluation. PCSR typically defines the safety envelope prior to pre-

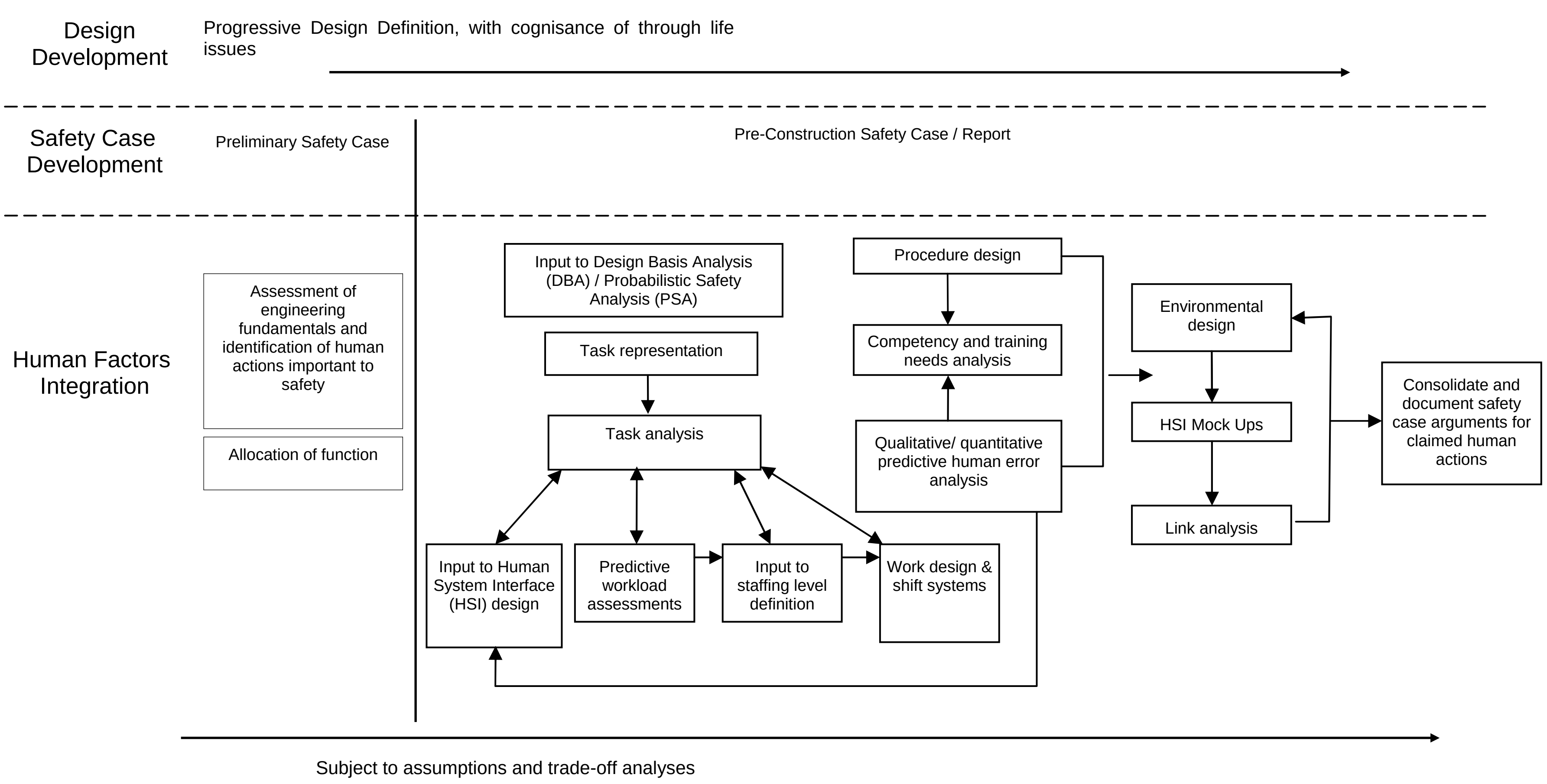
commissioning, therefore it is appropriate that the safety analysis supporting the design and operability of the proposed NPP is in place prior to the start of any (inactive) commissioning activities.

38 However, I recognise that the level of detail of HF analysis that can be undertaken for PCSR has a dependency on the reactor design development progress and the novelty of the engineered systems. I also recognise that at the PCSR stage a proportion of the HF analysis may be assumptions based and it will not be until later stage safety cases are developed that those assumptions can be validated and verified. However, this is not an argument to defer HF analysis as ordinarily it is possible to undertake assessment on the basis of expected (assumed) conditions, on a best estimate basis.

3.1.1.1 Human Factors in the Generic Design Assessment Pre-construction Safety Report

39 An important component of the GDA PCSR is that the reactor design is submitted for ONR assessment by a vendor / Requesting Party. This is particularly pertinent to HF as aspects of the [generic] HF safety submission are controlled / ‘designed’ by the licensee organisation, such as the strategy and type of procedures, the detail of the training regimes and the work design (including shift systems) and staffing levels. Therefore, for a generic safety submission, the RP can only propose strategies in these areas to underpin the generic risk assessment and ensure that those assumptions are transparent, such that any subsequent changes by the licensee organisation are clear. The Phase 2 risk assessment will then have to re-evaluate the impact of any changes and provide a revised safety demonstration.

Figure 1: Human Factors Analysis Expectations for Pre-Construction Safety Report


Design Development
Progressive Design Definition, with cognisance of through life issues
Safety Case Development
Preliminary Safety Case
Pre-Construction Safety Case / Report
Human Factors Integration
Assessment of engineering fundamentals and identification of human actions important to safety
Allocation of function
Input to Design Basis Analysis (DBA) / Probabilistic Safety Analysis (PSA)
Task representation
Task analysis
Input to Human System Interface (HSI) design
Predictive workload assessments
Input to staffing level definition
Work design & shift systems
Procedure design
Competency and training needs analysis
Qualitative/ quantitative predictive human error analysis
Environmental design
HSI Mock Ups
Link analysis
Consolidate and document safety case arguments for claimed human actions
Subject to assumptions and trade-off analyses

3.2 Generic Assessment Plan

40 The HSE '….Guide to Requesting Parties' (Ref. 5) describes GDA Step 4 as the *'detailed design assessment phase*', which aims to:

- Confirm that the higher level claims….are properly justified.
- Complete a sufficiently detailed assessment to allow ONR to come to a judgement as to whether a Design Acceptance Confirmation (DAC) can be issued.

41 The RP is required to submit a demonstration that:

- Construction and installation activities will result in a plant of appropriate quality.
- The constructed plant will be capable of being operated within safe limits.
- Arrangements are in place for moving the safety case to an operating regime.

42 Table 3 highlights the commitments provided by HSE for my GDA Step 4 Assessment Report and how the HF assessment makes a contribution to these commitments.

Table 3: Generic GDA Step 4 Assessment Requirements and Human Factors Considerations

Generic Step 4 Requirements	HF Consideration
Consideration of issues identified in Step 3.	Refer to Section 3.2.2 of this report
Judging the design against SAP and whether the proposed design reduces risks to ALARP.	Refer to Section 3.2.5, 3.2.6, 3.2.7, 3.2.8 and 3.2.9 of this report
Inspections of the RP's procedures and records.	N/A for HF
Independent verification analyses.	Refer to Sections 3.2.5 and 3.2.6 of this report
Reviewing details of the design controls, procurement and quality control arrangements to secure compliance with the design intent.	N/A for HF – covered by the Quality Assurance (QA) assessment function
Establishing whether the system performance and reliability requirements are substantiated by the detailed engineering design.	Refer to Sections 3.2.7, 3.2.8 and 3.2.9 of this report
Assessing arrangements for moving the safety case to an operating regime.	Refer to Section 4.5 of this report
Assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final design, building and construction.	Typically this is dealt with by the Verification and Validation programme post PCSR; as part of the Pre-Commissioning Safety Report (PCmSR).
Judging whether significant site parameters are appropriately defined in the generic site envelope.	N/A for HF
Reviewing overseas progress and issues raised by overseas regulators.	Refer to Section 4.7 of this report
Considering unresolved issues raised through the public involvement process.	No issues raised for HF
Resolution of identified nuclear safety issues, or identifying paths for resolution.	Refer to Section 5.4 of this report

43 My GDA Step 4 Assessment Plan for the UK EPR (Ref. 1) describes the overall assessment strategy for HF, which comprises 5 work streams. The numbering of the five work streams as presented in this report differs from that presented in the Assessment Plan (Ref. 1). This reflects only a restructuring of the order of presentation to maximise synergies between certain work streams and has no effect on the technical content. This approach was developed to ensure the proportionate targeting of my assessment to risk important human actions, to deliver appropriate coverage of the totality of HF technical areas and to probe EDF and AREVA's HF processes and procedures and from this sampling based process to give us a level of confidence in HF analyses that I have not targeted for detailed assessment. I also focused on engineered systems and operational approaches that I consider novel in the UK nuclear power plant context, to ensure that an appropriate consideration has been given to HF issues in the design thereby helping me form a judgement on whether EDF and AREVA have reduced the human error potential to ALARP. It should also be noted that not every aspect of my assessment has been undertaken to the same level of detail; this reflects the targeting and proportionality of my assessment process. Overviews of the five work streams along with the scopes and methodologies are provided in Sections 3.2.5, 3.2.6, 3.2.7, 3.2.8 and 3.2.9.

44 The five work streams were progressed as individual programmes of work addressing their particular assessment areas. However, several crossovers were apparent between work streams along with instances where the results of assessment activity from one work stream were beneficial to another (e.g. clarification on the design of the Main Control Room (MCR) and its equipment within Work Stream 5 providing informative input to Work Stream 1 Assessments). To maximise the benefit of crossovers and to eradicate duplication of effort, communication between assessment team members working on different work streams was frequent. In addition to general ongoing communication amongst the assessment team, monthly progress meetings were held during GDA Step 4 to provide an official forum for interaction between work streams. For additional detail see Section 3.2.10.

3.2.1 Generic Standards and Criteria

45 SAPs (Ref. 4) have formed the basis of the HF assessment. The SAP [preamble] require *'…assessments of the way in which individual, team and organisational performance can impact upon nuclear safety should influence the design of the plant, equipment and administrative control systems. The allocation of safety actions to human or engineered components should take account of their differing capabilities and limitations. The assessment should demonstrate that interactions between human and engineering components are fully understood and that human actions that might impact upon nuclear safety are clearly identified and adequately supported'.* All of the HF SAP (EHF.1 – EHF.10) apply to my Step 4 assessment. In addition the following SAPs are of principal relevance: SC.4, EKP.3, EKP.5, ESS.8, FA.9, FA.13 and FA.14.

46 The latest revision of the SAP is consistent with the International Atomic Energy Agency (IAEA) Standards and the Western European Nuclear Regulators' Association (WENRA) Reference Levels (Ref. 8).

47 To supplement, interpret and amplify the SAPs, the HF TAG have been applied where available (Ref. 7).

48 The UK also applies the fundamental principle of reducing risk to ALARP. This principle is at the forefront of my assessment and my judgement on using the principles in the

SAPs is always subject to consideration of ALARP. In the area of HF, ALARP arguments are often not explicit; they are inherent in the establishment and use of relevant good practices and standards. Of relevance to this assessment is guidance in the TAG on the demonstration of ALARP, T/AST/005 (Ref. 7) which states that "*the good practice or standard should be up-to-date, taking account of the current state-of-the-art; any practice or standard more than a few years old, or not subject to active on-going monitoring and review or not written by acknowledged experts may be suspect.*"

49 The SAPs and TAGs employed as the main assessment basis for the five work streams are listed in Table 4 below:

Table 4: Safety Assessment Principles and Technical Assessment Guides used as an Assessment Basis for GDA Step 4 HF Assessments

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. 7). T/AST/051 – Guidance on the purpose, scope and content of Nuclear Safety Cases (Ref. 7). T/AST/063 – Human Reliability Analysis (Ref. 7).
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. 7).
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. 7). T/AST/058 – Human Factors Integration (Ref. 7). T/AST/059 – Human Machine Interface (Ref. 7).
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. 7). T/AST/058 – Human Factors Integration (Ref. 7).

Table 4: Safety Assessment Principles and Technical Assessment Guides used as an Assessment Basis for GDA Step 4 HF Assessments

Work Stream	Relevant HF SAP applied	Relevant non-HF SAP applied	Relevant TAG applied
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. 7).

3.2.2 Findings from Generic Design Assessment Step 3

50 My work at GDA Step 3 identified a number of issues (see Table 5). These were assessed further within GDA Step 4.

Table 5: GDA Step 3 issues considered further during GDA Step 4

Issue and Step 3 Report Reference	Step 4 Assessment Plan Reference
Scope of Pre Fault human errors considered, para. 33	Sections 4.3.1 and (4.3.5 implicit)
Dependency modelling, para. 34	Sections 4.3.1 and (4.3.5 implicit)
Human Error contribution to initiating events, para. 36	Sections 4.3.1 and 4.3.5
Analysis of non credited post fault actions performed <30 minutes after fault occurrence, para. 37	Sections 4.3.1 and (4.3.5 implicit)
Misdiagnosis, para. 39	Sections 4.3.1 and (4.3.5 implicit)
Post fault action scope (beyond MCR), para. 40	Sections 4.3.1 and (4.3.5 implicit)
Use of Human Reliability Assessment (HRA) techniques, paras 41 and 50	Sections (4.3.1 implicit) and 4.3.5
Scope and availability of supporting HF analysis work, paras 45 and 46	Sections 4.3.2, 4.3.3 and 4.3.4
Substantiation of Human Error Probabilities (HEPs), para. 47	Sections 4.3.1, 4.3.2, 4.3.3 and 4.3.4
Suitability of standards base employed, para. 48	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4 and 4.3.5

Table 5: GDA Step 3 issues considered further during GDA Step 4

Issue and Step 3 Report Reference	Step 4 Assessment Plan Reference
Population Stereotypes, para. 55	Sections 4.3.2 and 4.3.4
Human Factors Engineering (HFE) Programme, paras 55 and 57	Sections 4.3.2 and 4.3.4
Competence and extent of HF team for UK EPR, para. 56	Section 4.3.4
Plant Overview Panel (POP), para. 60	Sections 4.3.1, 4.3.2 and 4.3.3
Alarm handling, para. 61	Sections 4.3.2 and 4.3.3
Soft controls, para. 62	Section 4.3.2
Computerised procedures, para. 63	Section 4.3.2
International regulatory liaison, para. 64	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4 and 4.3.5

3.2.3 Additional Areas for GDA Step 4 Human Factors Assessment

51 As my GDA Step 3 Assessment Report focused principally on identification of the human based safety claims for the UK EPR, the majority of my GDA Step 4 scope is in addition to resolution of issues identified by my GDA Step 3 Assessment Report.

3.2.3.1 Consideration of Design Specific Human Factors Issues

52 The UK EPR is an evolutionary Pressurised Water Reactor (PWR) design, based on recent German (Konvoi) and French (N4) series of 4-loop PWR plants. In particular, the design of the control room has been informed by EDF experience of the N4 control room, which makes considerable use of computerised display technology. the following design features of the UK EPR have informed by assessment approach.

Design to Reduce Sensitivity to Operator Errors

53 Chapter 3 of the November 2009 PCSR (Ref. 17) states that the design requirements for the UK EPR are intended to reduce the sensitivity of the plant to operator errors and reduce the reliance on operator actions for safety system actuation This is achieved by:

- Automatic control and by the provision of sufficiently large coolant capacity in the primary and the secondary systems, and in the primary and secondary feed systems to give adequate grace times for operator actions.
- Increasing design margins and use of passive systems, or systems using more passive features.

- Improvements to the Human Machine Interface (HMI) so as to provide the operators with additional reaction time and reliable information to diagnose the actual plant behaviour.

54 However, it is important to ensure that the increase in use of automatic control is appropriate and does not introduce new issues such as reduced situational awareness. The increase in reliance on passive systems and features, and reduced reliance on operator actuation of safety systems, potentially shifts the reliance on human action and vulnerability to human error to maintenance activities (including calibration, testing and surveillance). Therefore, I have ensured that Allocation of Function (AoF), automation and maintenance activities are targeted in my assessment.

Use of Computerised Technology

55 The UK EPR applies advanced computerised technology extensively, particularly in the MCR and generally to a greater extent than for current UK NPPs. The UK EPR control room features include:

- Computerised display technology.
- Large screen display panels.
- Computerised procedures.

There are a considerable number of HF issues relating to the use of computerised technology including (but not limited to):

- Operator situational awareness.
- Identification and response to failed or degraded systems.
- Display ergonomics.

Consequently, computerised technology has been an important consideration in my assessment. This has included consideration of the potential importance of software maintenance to safe plant operation.

Use of State Orientated Procedures and Automatic Diagnosis

56 The reference design for the UK EPR is FA3 and much of the HF safety case presented makes claims on both the SOA Procedures and supporting AD feature that forms a key part of the HMI alarm system. The SOA procedures for post-fault operation are based on those applied in all current French NPPs; and were originally developed as part of EDF’s response to the Three Mile Island accident. They are unique to EDF although they do have some similarity with Critical Safety Function based approaches. SOA procedures are intended to be a robust response to faults and EDF and AREVA claim they reduce the requirement for detailed event diagnosis. Using SOA, the required responses are based on the continual monitoring of a limited set of key safety functions. A limited set of SOA procedures are claimed by EDF and AREVA to be sufficient to deal with all accident situations unless severe accident conditions (i.e. core damage) occur.

57 The HMI for FA3 has been specifically tailored for use with SOA procedures during accident and emergency operation, as well as for normal operation and the substantiation of some key HRA claims are reliant on claims made for their use.

58 EDF and AREVA have incorporated a specific novel feature to the UK EPR to assist in the implementation of the SOA procedures. This is the AD feature that forms part of the overall alarm system. It undertakes continuous assessment of key safety functions and alarms when entry into SOA procedures are required, or when a shift between different

SOA procedures is required. It provides a summary of key plant conditions and directs the operators into the appropriate initial SOA. This feature has, in part, stemmed from experience gained from N4 plant and is intended to significantly reduce the 'diagnosis' burden on operators.

59 The AD potentially has both positive and negative impacts on human performance. It may reduce human errors from misdiagnosis and monitoring plant conditions during fault conditions. However, there may be issues such as:

- Increased reliance by operating staff on the system and reduced detailed knowledge of the plant behaviour.
- Identification of degradation or failure of the AD or the Process Information and Control System (PICS) system that it uses.
- Post-fault operation from either the PICS panels, or transfer to and use of the Safety Information and Control System (SICS) panel when the PICS system is not operable.

60 Consequently the use of SOA procedures and the role of the AD in supporting their reliable implementation are key areas of my assessment, particularly for the substantiation of key human based safety claims (Work Stream 1) and the overall ALARP assessment.

Operating Team Roles

61 The UK EPR has been designed around a differing operating concept than is currently applied in the UK. This concept employs a strategy operator (OS) and an action operator (OA) – rather than the typical reactor operator / secondary side operator roles. This has stemmed from trials conducted for FA3 and is judged by EDF and AREVA to offer a variety of benefits including better workload allocation and improved human error recovery by the operators. There is also a supervisor (SS) and safety engineer (SE) that completes the MCR team for fault operations.

62 At the onset of a fault, the supervisor and then safety engineer monitor plant conditions from the SICS panel. This is claimed to provide diversity and a potential means of recovery from significant errors made by operators. The detailed PICS HMI design, displays and procedures have generally been developed to support this operating concept. However, I note that the SICS panel is designed in a traditional manner (reactor panel, secondary side etc.). This may not support the same division of roles (OS, OA) as well due to the need for attention and actions to be undertaken over all control panels by both operators.

3.2.4 Research

63 The main area of research work I commissioned relates to human reliability data for interactions with digital systems, to inform the Work Stream 2 assessments. This is reported in Section 4.3 of this report.

64 In addition, I consulted the Organisation for Economic Co-operation and Development (OECD) Halden Reactor Project's reports database and reviewed their research material to determine relevance to my assessment. I also undertook a very high level review of ND's Nuclear Research Index for material that may be applicable to my assessment. The output of this work is embedded into my ALARP considerations as it has informed my assessment of EDF and AREVA's application of relevant good practice.

3.2.5 Work Stream 1: Substantiation of Human Based Safety Actions

65 This work stream is focused on ensuring that the risks from human actions have been reduced to ALARP. It is the foundation for my risk informed assessment and supports the GDA assessment strategy of considering the claims, arguments and evidence. The overriding aim of this area of my assessment is to ensure the adequacy of the identification and substantiation of important operator actions. Subsidiary to this, the work stream aimed to provide a judgement on:

- The completeness of the statement of ‘claims on the operator’.
- The adequacy of the justification, or process, intended to ensure that claims are reasonable and will be achievable by the realised design.
- Recommendations on any key area of follow-on work and assessment that is required to ensure that key claims are substantiated.

3.2.5.1 Standards and Criteria

66 The principal criterion for this aspect of my assessment is EHF.10 (Ref. 4): *“Risk assessments should identify and analyse human actions or omissions that might impact on safety”*. Also of particular relevance for Work Stream 1 are SC.4, EKP.1, EKP.4, EHF.2, EHF.3, EHF.5, EHF.6, EHF.10 and FA.7 (Ref. 4). TAG employed during the Work Stream 1 assessment were T/AST/005 – ND Guidance on the demonstration of ALARP (Ref. 7); T/AST/051 – Guidance on the purpose, scope and content of Nuclear Safety Cases (Ref. 7); and T/AST/063 – Human Reliability Analysis (Ref. 7). Additional guidance employed is provided in Ref. 5.

3.2.5.2 Scope and Method

67 Due to the absence of relevant detailed analysis and the late submission of information during the GDA Step 4 programme (Section 2 refers), I was not able to undertake the extent of assessment originally planned (Ref. 1). Instead my assessment for this work stream focused on testing the apparent assumptions within EDF and AREVA’s analysis and examining in detail the four task analyses provided by EDF and AREVA during GDA Step 4 (see Section 2).

68 The resulting Work Stream 1 Programme had two elements:

<u>(1) Initial Assessment of Claims and Assumptions Testing</u>

69 The activity during this element addressed the:

- Completeness of the statement of ‘claims on the operator’ made by EDF and AREVA.
- Adequacy of the submission in identifying all key claims.

70 I highlighted at GDA Step 3 that the UK EPR HRA was incomplete in terms of the human errors modelled. However, I sought additional evidence regarding error identification throughout Step 4.

71 As a check on the level of completeness, in the absence of extensive task analysis of claimed human actions, safety-related and safety-critical assumptions (both explicit and implicit) were logged as they became apparent within the UK EPR documentation. With the limited information available, it was not practical to subject the identified assumptions to formal Human Error Identification (HEI). As a result, my assessment was more

heuristic in nature by considering whether there were any assumptions that might be vulnerable to human error and which might represent analytical incompleteness.

(2) Assessment of the Detailed Substantiation of Claims on Human Based Safety Actions

72 My assessment in this area has been far less extensive than anticipated due to the very limited amount of comprehensive substantiation provided by EDF and AREVA. I performed thorough assessments of the substantiation of the four operator actions for which EDF and AREVA provided detailed task analyses during GDA Step 4.

73 My assessment of the four detailed task analyses applied a consistent approach to ensure completeness and comparability. In addition, the approach ensured that I undertook a rigorous, evidence-based assessment to inform my judgement on the adequacy of the EDF and AREVA substantiation of the analysed human based safety claims. I was specifically interested in whether:

- The claimed action been substantiated.
- The substantiation was adequate for the claimed action and the risk associated with the claimed action.
- The methods that have been applied by EDF and AREVA were appropriate to the claimed action.
- The associated HEP represented a realistic numerical value based on the information reviewed.
- The claim appeared to be ALARP.
- This assessment raised issues about the EDF and AREVA process for substantiation.
- EDF and AREVA's methods been applied in a systematic manner.

3.2.6 Work Stream 2: Generic Human Reliability Assessment

74 Work Stream 1 aims to assess in detail the substantiation of the HRA and, to a certain extent, Work Streams 5 and 3 also support the assessment of the HRA substantiation. Work Stream 2 aims to look generically at particular aspects of the HRA across the safety submission, particularly relating to HRA methods and application. Work Stream 2 will also reach a judgement on the general acceptability of the HEPs proposed against task types and continue the assessment of the HRA carried out for GDA Step 3 from both the PSA and HF technical areas.

3.2.6.1 Standards and Criteria

75 The principal criterion for this aspect of my assessment is EHF.10 (Ref. 4): *"Risk assessments should identify and analyse human actions or omissions that might impact on safety"*. The supplementary text to EHF.10 relates directly to the components of Work Stream 5, most notably stating that *"The selection and application of probability data for human errors should be:*

76 *a) derived from operational experience data and/or through the application of recognised human reliability assessment techniques. Use of either approach should be justified and its relevance for the task and context demonstrated."*

77 Also *"Risk assessments should directly model dependent human errors committed by a single operator or different operators."*

78 In addition the assessments considered SAP SC.5, ERL.1, EHF.5, EHF.7 and FA.13 (Ref. 4). The assessments also employed TAG T/AST/063 – Human Reliability Analysis (Ref. 7).

3.2.6.2 Scope and Method

79 This area of my assessment was divided into four components:

(1) The Relevance of Extant HRA Techniques for the Assessment of Modern Control Room Task Environments

80 My assessment focused on the relevance and suitability of HEPs contained within the HRA techniques developed in the era of hard wired control interfaces, for use in PSA of contemporary control rooms which are more heavily reliant on human-computer interfaces.

81 I undertook a significant literature review to support this work, focused on obtaining data that provides insights into human reliability issues associated with human computer interfaces. I considered the sensitivity of the data to the context within which the data has been gathered and whether that data is judged to be strongly dependent upon artefacts that arise as a function of the systems under control, or the interface system from which the data has been derived.

(2) Assessment of Level 1 and Level 2 PSA

82 The HRA for UK EPR applies (the) ASEP (Ref. 26) to perform a screening assessment for the level 1 PSA. Subsequently, for the level 2 PSA, best estimate HEPs were derived using the SPAR-H (Ref. 27) method. Therefore, the issue arises whether the use of the two approaches is internally consistent with regard to the information used, and valid in principle. In practice, the fundamental issue is whether the human interactions pertinent to risk have been properly identified and addressed, irrespective of the approach used.

(3) Assessment of Dependency Treatment

83 In this area I have provided a judgement on the adequacy of the techniques employed and their method of application in the treatment of dependency within and between *HFE*s[2] contained within the RP's HRA for both the Level 1 and Level 2 PSA. This component of my assessment had two elements:

84 (i) *Identification of current good practices for the treatment of human error dependencies*. This was undertaken via literature review to identify appropriate good practice from regulatory bodies, academic research and other internationally recognised organisations. I considered the treatment of dependency within particular HRA techniques, including those used by EDF and AREVA, in order to inform my assessment of the treatment of dependency used in the UK EPR HRA.

85 (ii) *Evaluation of the modelling of dependency within the PSA.* EDF and AREVA's accommodation of Human Error Dependence (HED) was assessed for both Level 1 and Level 2 PSA. I reviewed all *HFE* dependency level allocations to identify the claims made in relation to HED, evaluate the underpinning arguments and finally to evaluate the evidence provided to support the argument.

[2] When referring to Human Failure Events the abbreviation is italicised (*HFE*) to distinguish between Human Failure Events and Human Factors Engineering

86 I also reviewed the CDF cutset analysis in order to identify those cutsets with multiple HFE and to determine that the level of human reliability claimed in the cutset does not exceed that prescribed by Human Performance Limiting Values (HPLV).

(4) Assessment of the Use of the Human Cognitive Reliability Technique for Long Timescale Recovery Activities in the Spent Fuel Pool

87 I considered the application of the Human Cognitive Reliability (HCR) technique for the assessment of long timescale recovery tasks in the spent fuel pool. The application of this technique is a departure from the other HRA methods employed by EDF and AREVA for the PSA.

88 I undertook a technical review of the application of the HCR method and its general appropriateness for use in the context applied by EDF and AREVA.

3.2.7 Work Stream 3: Engineering Systems

89 Work Stream 3 focused on system / equipment maintenance[3]. This work stream is important to ensure claims and assumptions about the reliability of systems and components are adequately underpinned. The particular focus of the work stream was general maintenance reliability. This included inspection, calibration and testing (at a strategic level - for example the general approach to ‘maintenance’).

3.2.7.1 Standards and Criteria

90 A number of SAPs were considered as criteria for the Work Stream 3 assessments. Of particular importance is EHF.3 (Ref. 4) which requires that *“A systematic approach should be taken to identifying human actions that can impact on safety”*. In addition to this a several other SAP have a direct relevance and were employed during the assessment. These are MS.4, SC.7, EKP.3, ECS.3, ECS.5, ERL.2, EMT.1, EMT.4, EMT.6, EMT.7, ELO.1, EMC.3, EMC.8, EMC.13, EMC.27, EMC.28, ESS.3, ESS.12, ESS.15, ESS.21, ESS.22, ESS.26, EHF.1, EHF.2, EHF.3, EHF.6, EHF.7 and EHF.10 (Ref. 4). The following TAG were applied to the assessment; T/AST/009 – Maintenance, inspection and testing of safety systems, safety-related structures and components (Ref. 7); T/AST/058 – Human Factors Integration (Ref. 7); and T/AST/059 – Human Machine Interface (Ref. 7).

3.2.7.2 Scope and Method

91 My focus for this work was to ensure that those safety systems with the most significant risk impact have been analysed for the human error potential during maintenance activities. I also generically reviewed factors that can affect maintenance performance (local to plant conditions including the working environment and physical access for example) and the use of Operating Experience Feedback (OEF) to support the EDF and AREVA maintenance human error analysis, and to inform the design for maintainability of systems. The topics addressed were:

- General maintenance.
- Design for maintainability.

[3] ‘Maintenance’ activities include physical testing and manipulations, surveillances, monitoring and outage related activities.

- Reactor Building / Containment access.
- Workspace (physical access for maintenance tasks).
- Software maintenance.
- Use of OEF.

92 The assessment work for Work Stream 3 was performed in two phases.

Phase 1 – Identification and High Level Overview of Maintenance Related HF Claims

93 This aspect of my assessment aimed to identify what claims are made on operators with regard to maintenance, and to establish what evidence is available to support the identified claims.

Phase 2 – Detailed Examination of Identified HF Claims Related to Maintenance

94 I aimed to consider, in detail, a selection of claims identified as part of the Phase 1 work and I particularly focused on general maintenance and the use of OEF.

95 My phase 1 initial review indicated that the topics of particular interest were:

- The use of operational experience.
- General maintenance.

3.2.8 Work Stream 4: Human Factors Integration

96 The focus of this work stream is the general processes and mechanisms in place to deliver quality HF input to the design of the UK EPR and the safety case for the UK. This is particularly important in light of the UK's sampling and targeted approach to assessment. As my approach does not assess the entirety of a safety submission, this work stream aims to provide us with a level of confidence or otherwise that the HF analyses, not assessed during GDA, are of a suitable quality to inform the design and safety submission and ultimately to support reliable human intervention.

3.2.8.1 Standards and Criteria

97 The principal criterion for this aspect of my assessment in this area was EHF. 1 (Ref. 4): *"A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the entire facility lifecycle."* Further to this the other HF SAP (EHF.2 – EHF.10) (Ref. 4) represent the totality of necessary HF consideration during the design, development and operation of a nuclear plant. I also used TAG T/AST/058 - Human Factors Integration (Ref. 7) during the assessment. The standards I have employed are provided in Refs 77, 78, 79, 80 and 81.

3.2.8.2 Scope and Method

98 My assessment in this area covered three main topics: the organisation, process and implementation of HF. This resulted in five work components:

(1) Establish Standards and Good Practice in the Area of HFI

99 I identified and reviewed a variety of good practice sources to establish an appropriate baseline against which to assess EDF and AREVA's approach to HFI.

(2) Assess EDF and AREVA's Reported Standards and Guidance Against Good Practice Baseline

100 I undertook a high level 'face value' assessment of the HF standards and guidance claimed by EDF and AREVA to have been applied to their design and safety analysis of the UK EPR, against my baseline.

(3) Assess EDF and AREVA's Organisation for HFI

101 I considered the location of the HF team within the organisation to assess whether it was suitably embedded and had a sufficiently broad focus to be able to influence decision making across the project, the authority of the team to influence the design and the competence of those undertaking the HF work.

(4) Assess EDF and AREVA's Processes for HFI

102 HFI in the UK is typically driven via a Human Factors Integration Plan (HFIP) and a suite of HF safety management processes. This area of my assessment aimed to consider the EDF and AREVA HFIP or equivalent.

(5) Assess EDF and AREVA's Implementation of HFI

103 This aspect of my assessment sought high level evidence of the implementation of the standards and guidance claimed to have been applied by EDF and AREVA.

3.2.9 Work Stream 5: Plant-wide Generic Human Factors Assessment

104 This work stream complements Work Stream 1 and assesses generic HF issues that would not necessarily be highlighted as part of Work Stream 1. Whereas Work Stream 1 considers the depth of HF analyses, Work Stream 5 aims to assess across the breadth of HF analyses in order to provide a judgement on the adequacy of the overall plant ergonomics and how well the plant design meets modern standards and adopts recognised good practice. It is an important area to ensure that the design meets ALARP requirements.

105 The Work Stream 1 assessment uses the output (or 'results') of technical HF areas reviewed under Work Stream 5, but only relating to individual human actions (to the extent possible given the limited substantive material provided). For example, I considered the human-computer interface (HCI) and alarm philosophy generically during Work Stream 5 and will consider the output of that philosophy in terms of individual interfaces and alarms to support specific operator actions during Work Stream 1.

106 Work Stream 5 is not necessarily risk informed and aims to ensure the supportability and consistency of general tasks – these tasks underpin reliable human intervention. In doing so the work stream considers the central control room specifically and local to plant work areas as appropriate.

3.2.9.1 Scope, Method of Assessment and Standards and Criteria

107 Work Stream 5 is plant-wide and considers seven discrete assessment areas. The particular SAP, TAG and other guidance material used as an assessment base are defined in the following subsections.

108 The intention is to assess all the main aspects of the UK EPR that could impact human performance against appropriate HF criteria, with a specific focus upon features that could increase the potential for human error.

109 Particular SAPs considered during the Work Stream 5 assessments were ESS.8, ESS.9, EHF.2, EHF.5, EHF.6, EHF.7, EHF.8 and EHF.9 (Ref. 4).

(1) Allocation of Function

110 Effective AoF should ensure that tasks are allocated between humans and systems to account for their relative strengths and limitations. Where processes are automated, I have sought to ensure that the operator can maintain an appropriate level of situation awareness, which is particularly important should the automated systems fail and require restorative operator input. In addition, an appropriate allocation of function should not result in an unacceptably high or low workload. For the purposes of my assessment, automation is deemed to include automatic control of parameters, automatic process sequences, automatic safety protection, mechanical or electrical interlocks or key exchanges, alarm management and computerised procedures.

111 The principal criterion for this aspect of my assessment was SAP EHF.2: *“when designing systems, the allocation of safety actions between human and technology should be substantiated and dependence upon human action to maintain a safe state should be minimised.”* I also considered SAP ESS.8 and ESS.9. My assessments used available documentation describing both the AoF process followed by EDF and AREVA and also design documentation providing details of the results of this process. As well as examining the documentation, AoF was discussed in detail with relevant EDF and AREVA staff during a three-day meeting at the EDF simulator facility in Paris.

112 Initial assessment work for this component focused on identifying claims made regarding AoF by EDF and AREVA and exploring their stated functional allocation process. A sample of four safety-related scenarios was then selected for assessment. Evidence was sought on whether the functional allocations, within the systems used for these scenarios, followed the previously identified methodology and provided appropriate AoF.

(2) Physical and Environmental Ergonomics

113 Optimising the physical design of work spaces and working environments is important to ensure that they do not adversely impact human performance.

114 The principal criterion for this aspect of my assessment was EHF.6: *“workplaces in which plant operators and maintenance is conduced should be designed to support reliable task performance, by taking account of human perceptual and physical characteristics of the impact of environmental factors.”* In addition other guidance sources used were provided by Refs 10, 82, 83, 84 and 85.

115 My assessment addressed a variety of locations throughout the plant with a sampling approach applied where necessary. These were:

- MCR.
- Remote Shutdown Station (RSS).
- Fuel Handling Facility.
- Local-to-plant interfaces.
- Maintenance locations.
- Access routes.

116 For each location assessed, I considered the lighting, heating and ventilation, noise, and the physical arrangement of workspaces. Within these assessments, varying plant conditions were considered including routine operations, maintenance and abnormal /

emergency conditions. I took advantage of any task analyses available for actions located in the workspaces assessed and where habitation/access was infrequent, I relaxed my assessment detail on a proportionate basis. The basis of my assessment for this component was a combination of EDF and AREVA technical drawings, design documentation and information gathered during discussions with EDF and AREVA personnel and visits to the FA3 simulator.

(3) Control and Display Interfaces Including Alarms

Control and display interfaces should be designed and arranged in a manner that supports personnel in the efficient and reliable undertaking of safety-related tasks.

117 The principal criterion for this component is EHF.7: *"user interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all states"*. SAP EHF.6 was also considered along with ESR.1. TAG T/AST/059 – Human Machine Interface (Ref. 7) presents ONR's expectations with regard to HMI design and I have applied these expectations to my assessment. The principal external guidelines applied are cited in Refs 10, 86 and 87. Assessment was performed via technical drawings and screen formats, as appropriate, along with observation in the EPR simulator facility.

118 My assessment focused on control and display interfaces provided within the MCR as there was very little information relating to interface design outside of the MCR. However, I note that it is intended that certain interfaces be replicated in alternate locations (e.g. Remote Shutdown Station (RSS)) and therefore my assessment will apply equally there. The interfaces I considered were both computer based and conventional:

- PICS (routine operations).
- Plant Overview Panel (POP) (routine operations).
- Hard wired controls at OS/OA workstations.
- SICS (post fault operations).

119 My assessment also included the associated alarm systems related to the controls and information displays used to operate and monitor the plant.

(4) Work Organisation

120 Detailed examination of this component is not appropriate until GDA Phase 2, as the specific work organisation and staffing levels will be determined by the licensee organisation. However, assumptions relating to these areas are made in the GDA risk assessment relating to the MCR and it is on this basis that I have sought some assurance of the suitability of the proposals and the impact of them on human performance. Any licensee changes to the arrangements applied for GDA analysis will require re-assessment during Phase 2. My focus here has been on reviewing how EDF and AREVA have derived their staffing levels and assessed workload.

121 The supplementary text to SAP EHF.5 [which defines my expectations for task analysis] states that the task analysis *"….should be sufficiently detailed and demonstrably employed, to provide a basis for…..defining staffing levels…"* and *"the workload of personnel required to fulfil safety-related actions should be analysed and demonstrated to be reasonably achievable"*. These criteria have formed the basis of my assessment in this area.

(5) Procedures

122 Detailed examination of this component is not appropriate until GDA Phase 2, as the specific strategy, type and format of the range of procedures will be determined by the licensee organisation. However, the GDA risk assessment makes assumptions relating to the use of the SOA for addressing faults and accident scenarios, which is a different approach to existing practice within UK NPP operation. It is on this basis that I have sought assurance of the suitability of the proposals and the impact of them on human performance. Any licensee changes to the proposals made for GDA will require re-assessment during Phase 2.

123 The principal criterion used for my assessment is EHF.9: *“procedures should be produced to support reliable human performance during activities that could impact on safety.”* In support of this EHF.4 states that *“Administrative controls used to remain within the safe operating envelope should be systematically identified”*. It goes on to state that *“The design of these controls should be such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.”*

124 I have undertaken a high level general assessment of the use of procedures. Ordinarily the PICS computer interface is used to present procedures. Should the PICS fail, paper based procedures are used (with control and display functionality provided by the SICS).

125 A sample of procedures were assessed (computer and paper based). In absence of guidance from a relevant TAG (at the time of writing), I focused on the following general aspects of procedure design:

- Place keeping, to ensure that task steps are not omitted.
- Checking, to ensure that safety important task steps are verified.
- How the procedures support reliable plant parameter monitoring and sustained vigilance.
- Situational awareness and completeness of the information provided.

126 I particularly focused on the following elements of the SOA and its associated procedures:

- The reliance on the automated diagnosis (AD) and the means by which the operators check the diagnosis, and the diverse method of undertaking fault diagnosis on AD failure or degradation;
- The combined use of paper based procedures and computer based procedures for strategy and detailed action implementation, to determine their impact on the claims for operator actions;
- The separation of activities between a strategy operator (OS) and action operator (OA) for the implementation of the SOA, together with a third individual to undertake diverse monitoring of key safety functions via the SICS panel; and
- The transfer from PICS to SICS operation on PICS failure – this transition requires SOA implementation without the AD support and necessitating used of procedures tailored to the SICS conventional panel

3.2.10 Use of Technical Support Contractor(s)

127 Technical Support Contractors (*TSCs*[4]) were commissioned to undertake some of the assessment analysis work described in my assessment plan. Such additional resource was required due to the significant volume of assessment work committed to and the relatively short timescales involved.

128 My *TSC* comprised recognised experts in the fields of HF and HRA, some of whom are recognised world experts in their discipline. In addition, the majority of my *TSC*s were involved with the HF and HRA contribution to the Sizewell B (SZB) NPP. All of my *TSC*s are academically qualified in HF or HRA related areas and hold a significant number of years experience in the application of HF and HRA to NPP design and safety analysis. In addition, two of my team were previously nuclear safety regulators from the UK and the United States of America (USA). My principal *TSC* team was organised as a consortium of individuals under an ‘umbrella’ HF consultancy, which also acted as a management function for the *TSC*.

129 Each of the work streams had a nominated work stream lead assessor from the *TSC*; who was typically an accepted expert in that particular field, supported by a small team of other qualified assessors. The work stream leaders developed individual assessment plans to support my overarching assessment plan for GDA Step 4. These were based on technical specifications that I developed. They were then responsible for delivery of the scope of work against their plan and the technical accuracy and quality assurance of their resultant reports.

130 My *TSC*s produced Assessment Reports which were typically analysis of EDF and AREVA submissions, supplemented by visits to the EPR simulator. I closely directed and monitored the *TSC* work via weekly telephone conferences and monthly face-to-face meetings with the principal team. Their analysis and Assessment Reports were used to inform my regulatory judgements only. I was not directed or obliged to accept, or otherwise, information presented by the *TSC*. Use of their work was entirely at my own discretion and I have made my decisions and reached the judgements presented in this report based on a number of factors, including the work offered by my *TSC*s.

3.2.11 Regulatory Interactions with EDF and AREVA

131 During GDA Step 4, I had various interactions with EDF and AREVA. These were via formal written communication or meetings (in person and via telephone/video conference). My overall approach to interaction with EDF and AREVA was one of openness. I made particular effort to inform EDF and AREVA of my findings as they emerged, in order that they may take account of them in their ongoing work, particularly where this may improve their position for GDA Step 4.

3.2.11.1 Technical Queries and Regulatory Observations

132 Formal written communication was provided in the form of TQs and ROs to which EDF and AREVA were required to provide a written response. TQs provided a means for me to formally seek clarification or further information from EDF and AREVA. ROs enabled me to bring significant findings from my assessments to the notice of EDF and AREVA. Details of the scope and purpose of TQs and ROs are provided in “Interface Protocol

[4] When referring to Technical Support Contractors the abbreviation is italicised (*TSC*) to distinguish between Technical Support Contractors and the Technical Support Centre

between HSE Nuclear Directorate / Environment Agency and Requesting Parties", JPO/003 (Ref. 76).

133 There are 35 TQs relevant to my GDA Step 4 assessment.

134 EDF and AREVA's response to my TQs has not been completely satisfactory. Although there has been a willingness to respond, some of the responses have been late and some have not fully answered the queries posed. This appears to have been in part due to a lack of understanding of the UK regulatory expectations and in part due to resource problems. Overall, specific responses to 33 of the TQs have been provided with the other two being covered to some degree by responses to other TQs.

135 I raised four ROs on EDF and AREVA during GDA Step 4. A further RO raised during GDA Step 3 (RO-UKEPR-038) was carried over to GDA Step 4 as EDF and AREVA were unable to provide a response to it within GDA Step 3. The five ROs considered within GDA Step 4 are presented in Table 6 below.

Table 6: Human Factors Regulatory Observations considered during GDA Step 4

RO Number	RO description
RO-UKEPR-038	The current PCSR for the UK EPR does not present the safety case for HF in a recognisable UK structure. The UK regulators expect this to be addressed in response to the attached Regulatory Observation Actions (ROAs).
RO-UKEPR-059	The UK Regulators request access to an EPR simulator to facilitate the GDA Step 4 HF Assessment.
RO-UKEPR-071	ND considers that the PCSR and supporting submissions for GDA do not adequately consider maintenance induced human errors (or latent human failures/ Type A *HFEs*). There is a significant lack / complete omission of qualitative HF analysis to demonstrate that the risk from latent human failures has been reduced to ALARP. We acknowledge that there is some quantitative treatment of pre-accident human errors, but that is only focused on manual valves (as noted by ND in the GDA Step 3 report). ND considers that the UK EPR safety submission should include human factors analysis of maintenance activities on a proportionate basis to the risk presented by the corresponding safety system unavailability. This work is also linked to RO-UKEPR-038.
RO-UKEPR-079	The EPR design incorporates an AD feature that is intended to reduce the potential for misdiagnosis along with the SOA for fault procedures. However ND considers that the PCSR and supporting submissions for GDA have not provided an adequate justification that the potential for misdiagnosis has been demonstrated to be ALARP.
RO-UKEPR-080	ND considers that the PCSR and supporting submissions for GDA do not consider the potential for violations.

136 EDF and AREVA have provided a response to each of the five ROs during GDA Step 4. For both RO-UKEPR-038 and 071, EDF and AREVA's response has essentially been via a commitment to undertake work to address the identified gaps in their safety case. Some of this work has been submitted during GDA Step 4 (primarily four task analyses

for key claims) and is included in my assessment. The remaining work forms the foundation for of their resolution plan for the GDA Issue for the UK EPR.

137 Responses to RO-UKEPR-079 and 080 were received late in Step 4 (December 2010 and January 2011). However, I have undertaken an initial assessment of them as part of my Work Stream 1 assessment.

3.2.11.2 Meetings

138 I had numerous discussions with EDF and AREVA during GDA Step 4. These were undertaken for several reasons:

- Informing them of my assessment progress and emerging findings.
- Providing them with opportunity to inform me of their ongoing design and analysis work (particularly in response to my TQs and ROs).
- Undertaking technical inspections to further my assessment (e.g. visits to EPR simulator facility).

A schedule of these interactions is provided in Table 7 below:

Table 7: Human Factors meetings and discussions between ONR and EDF and AREVA during GDA Step 4

Date	Interaction
02/12/09	EDF PCSR Update.
10/12/09	Launch of GDA Step 4 with RPs.
07/01/10	Level 4 meeting held at EDF offices in Paris to discuss RO 38 and the links between the HRA and HFE programme.
08/01/10	Visit to EDF offices in Paris, France to observe the EPR simulator facility.
17/02/10 – 18/02/10	Level 3 meeting to discuss the HF safety case and apparent gaps from my early assessment.
01/04/10	Telecon to discuss general update and progress.
15/04/10	Level 4 meeting held at EDF offices in Paris, France to discuss task analysis methodology and examples.
03/06/10	Telecon to discuss task analyses and TA methods statement.
21/06/10 – 23/06/10	Visit to EDF offices in Paris, France to observe the EPR simulator facility.
24/06/10	Level 4 meeting held at EDF offices in Paris, France to discuss task analysis example and seek clarification on TA forward work programme.
21/07/10	Meeting to discuss EDF and AREVA’s approach to HF in the assessment of Internal Hazards, held at EDF offices in London.
24/08/10	Telecon to discuss ND comments on task analysis for start-up of station black out diesels following a loss of off-site power.
03/09/10	Meeting to discuss RO-UKEPR-070.
23/09/10	Telecon to discuss EDF and AREVA approach to HF in the assessment of Internal Hazards.

Table 7: Human Factors meetings and discussions between ONR and EDF and AREVA during GDA Step 4

Date	Interaction
6/10/10	Level 4 meeting held at EDF offices in Paris, France to discuss proposed responses to ROs 38 and 71.
7/10/10	Level 4 meeting on Internal Hazards held at EDF offices in Paris, France to discuss HF issues potentially arising from dropped loads and flooding.
2/11/10	Computer Aided Design (CAD) model visit and discussions held at EDF offices in Paris, France to discuss maintenance and HFI.
04/11/10	Convergence meeting. The convergence meeting was a specific GDA Step 4 event (similar meetings held by other assessment disciplines). It covered the following items: • confirmation of agreed GDA scope; • status of ROs and TQs; • emerging findings and conclusions from my assessment; and • further analysis work being undertaken by EDF and AREVA to support GDA Step 4 and post interim DAC phase.
03/12/10	Telecon to discuss Work Stream 4.
06/12/10	Telecon to discuss EDF and AREVA's response to TQ-UKEPR-1026 and others on HF integration.
08/12/10	Telecon to discuss out of scope items for GDA Step 4.
10/12/10	Meeting to provide feedback on my assessments and for updates on the progress of EDF and AREVA's analysis work (including responses to TQs and ROs).
07/01/11	Telecon to discuss draft HF GDA Issues and out of scope items.
12/01/11	Level 4 meeting held at EDF offices in London to discuss GDA Issue resolution plans and details of pre and post-fault task analyses to be undertaken.
20/01/11	Telecon to discuss GDA Issue 1.
21/01/11	Telecon to discuss EDF and AREVA's issues surrounding what is deemed to be out of scope for GDA Step 4.

3.2.12 Cross-Cutting Topics and Integration with Other Assessment Topics

139 HF is a Cross-cutting subject incorporating aspects of many engineering disciplines and as a result, requires integration with other assessment topic areas. My main interaction areas are described in Table 8 below:

Table 8: Cross-cutting assessment disciplines with human factors

Assessment Area	Interaction with HF

Table 8: Cross-cutting assessment disciplines with human factors

Assessment Area	Interaction with HF
Probabilistic Safety Analysis	This is the principle area of integration; with PSA and HF jointly leading the human reliability assessment discipline. I worked with PSA colleagues to understand the relative contribution of people and systems to the overall plant risk; which fed directly into my Work Streams 1, 2 and 3 assessments. PSA contributed to the selection of fault sequences considered for dependency assessments (Work Stream 2). In addition PSA colleagues assisted my understanding of those plant systems contributing significantly to risk; to focus my maintenance assessment work (Work Stream 3).
Fault studies	I worked with fault studies colleagues principally on potential safety case claims on operator actions for boron dilution and Steam Generator Tube Rupture (SGTR) faults as the case for these faults was developed for UK EPR.
Control and instrumentation	My principal integration with control and instrumentation related to software maintenance and safety system reliability and availability.
Internal hazards	Human actions associated with fires, floods and dropped loads were my focus. I have worked with my Internal hazards colleagues in the determination of both deterministic and risk mitigation claims for human actions in these areas.
Mechanical engineering	My principal integration with mechanical engineering has related to system and equipment maintenance to assist my maintenance assessment work (Work Steam 3).

3.2.13 Out of Scope Items

140 The following items have been agreed with EDF and AREVA to be out of scope for GDA:

- Team organisation.
- Staffing.
- Operating and maintenance procedures.
- Use of SOA.
- Display breakdown.
- Training.

141 Assumptions are made with regard to some of these aspects in the GDA risk assessment. However, the operational reality is not determined until GDA Phase 2 (site licensing). The final interface designs for the UK will not be available until Phase 2.

4 GDA STEP 4 ONR ASSESSMENT FOR HUMAN FACTORS

4.1 Structure of Section

142 My assessment is provided in line with the five individual work streams outlined in Sections 3.2.5, 3.2.6, 3.2.7, 3.2.8 and 3.2.9. My consolidated judgements are provided following consideration of the individual work streams.

4.2 Work Stream 1: Substantiation of Human Based Safety Actions – Assessment

143 Throughout GDA, EDF and AREVA have struggled to understand the UK requirements for HF safety cases and the requirement to demonstrate that the risk from human error has been reduced to ALARP. I agree with EDF and AREVA that this is largely a result of the difference in regulatory approaches to HF between the UK and France.

144 At the end of GDA Step 3, I concluded that the EDF and AREVA PCSR had not presented an adequate case for HF for the UK EPR and I raised RO-UKEPR-38 in response. Through regulatory exchange during the preliminary months of GDA Step 4, it became clear that EDF and AREVA did not have qualitative HF analyses of the type typically expected to underpin UK safety cases. EDF and AREVA advised that analyses of the type expected by UK Regulators would have to be developed specifically for the UK and that time and resource constraints limited what could reasonably be provided to support GDA Step 4. As a result, EDF and AREVA submitted four detailed task analyses and three method statements relating to my Work Stream 1 programme, and it is these that form the majority of my assessment, together with material submitted in relation to additional ROs raised throughout GDA Step 4. I consider the volume of material provided to underpin the HF safety case a minimal position, and as only four analyses were provided, there is a significant and substantial gap in the safety case for HF and RO-UKEPR-38 remains outstanding. I have therefore reflected this gap in GDA Issue **GI-UKEPR-HF-01**. The complete GDA Issue and associated actions are formally defined in Annex 2.

145 In the November 2009 PSCR, it is difficult to derive explicit pertinent safety claims relating to Work Stream 1 as the material is not presented in a claims, arguments and evidence framework. In fact there does not appear to be any overarching framework or context to the HFE programme. The most relevant statement, analogous to a safety claim, relates to the declared 'safety objectives' of the HFE programme: "….*A major objective of the HFE programme has been to take advantage of human capabilities, whilst minimising both the potential for human error and the impact of those errors on the plant*." In addition, in the narrative in Chapter 18.1 on the impact of HF on EPR safety, it is stated that "*In the EPR design the impact of human error on safety is minimised by the use of inherently self-regulated automation systems and passive response characteristics, which ensures that after a significant event has occurred no human action is required for at least 30 minutes, and no local to plant action is required for at least 60 minutes*". There are no related arguments and evidence presented in the November 2009 PCSR. The evidence base for this aspect of my assessment programme is the Level 1 and 2 PSA HRAs, the four qualitative task analyses developed for GDA and the material presented in response to my RO-UKEPR-079 on operator misdiagnosis and RO-UKEPR-080 on violations.

4.2.1 Identification of Human Based Safety Claims

146 At the end of Step 3, I commented that EDF and AREVA had presented a reasonably clear demonstration of the human contribution to risk via the HRA, although I noted some

omissions and weaknesses in the model. The PSA model that forms the basis for my assessment has not been revised since Step 3, hence my comments remain, although in Step 4, I have assessed more closely the derivation of the claims to inform my judgement on adequacy and completeness of the human based safety claims.

147 In the Level 1 PSA (2009) there are 187 Type A *HFEs* (pre initiating human errors), 5 Type B *HFEs* (human errors contributing to an initiating event) and 59 Type C *HFEs* (post fault human errors). The actions included in the model appear to have been derived from operating experience and there is no detailed description of the process for the (historical) identification of the claimed human actions. I do not consider this adequate as I expect to see a logical argument relating the (similarities and differences of) plant systems of the UK EPR to earlier plant designs, to demonstrate applicability of the claimed actions to the current design and to highlight that their risk contribution remains the same as earlier evolutions of the design. I have raised the following Assessment Finding (AF) on a future licensee to improve the safety case on this topic.

> ***AF-UKEPR-HF-01 –*** *The licensee shall ensure comprehensive identification of human based safety claims, and justify the relevance and applicability of the claims to the UK EPR as part of the HRA revision.*

148 In terms of Type A *HFEs*, I noted at GDA Step 3 that only manual valve alignments are modelled. Automatic valves realigned on system demand and manoeuvrable from the MCR have been screened out on the basis that unavailability would be revealed during routine plant surveillance. Calibration errors and failures during inspection and test, that result in systems being left in an unavailable or degraded state, have not been considered explicitly and are assumed to be adequately included into the equipment failure rates used for the PSA. Again, as I noted at GDA Step 3, this is not adequate and I expect that the contribution of human errors within the equipment failure rates to be highlighted (Ref. 6). I did not require this to be undertaken during GDA Step 4, as I recognised the intention to fully revise and update the PSA going forward post GDA Step 4. I considered it disproportionate to require a HRA revision during GDA Step 4 out with the PSA update, and it would not have provided any significant safety benefit at this stage. In particular, equipment procurement timescales are post GDA Step 4 and therefore there is time available for the required analysis (quantitative and qualitative) to feed into the design process and hence there is no foreclosing of options in this regard. Hence, I have raised the following AF (see Annex 1) on a future licensee.

> ***AF-UKEPR-HF-02*** *– The licensee shall explicitly highlight the human error probabilities associated with Type A HFEs as part of the Level 1 HRA revision.*

149 In terms of Type B *HFEs*, again the approach has been to use extensive operating experience and earlier safety studies. There is no explanation of the process for deriving these claims, or an argued demonstration of how they remain applicable to the UK EPR There is also no demonstration that cited Type B *HFEs* are complete.. Only five events have explicit HEPs and these are conservative values. I therefore consider that this aspect of the model may be incomplete and that a systematic analysis is required to demonstrate that the revised HRA includes a complete identification of the human error contribution to initiating events, particularly for low power and shutdown states (where human errors are typically more important contributors to risk). I have raised the following AF on a future licensee (see Annex 1).

> ***AF-UKEPR-HF-03*** *– The licensee shall undertake a systematic analysis to demonstrate that all credible Type B HFEs are included in the revised Level 1 HRA.*

150 For type C *HFEs*, there is limited information on how the actions have been derived: *"To determine those actions, typical PWR actions and operating procedures adapted to the EPR design have been used. Additional recovery actions have been identified using expert judgment of PSA and EOP experts"*. It is also stated that: *"Only the recovery actions are addressed for the GDA process, the actions of commission due to misdiagnosis are not modelled"*. Once again there is no evidence to demonstrate that the identified actions are a complete citation of the post fault operator requirement. It is clear however, that there is no consideration of aggravating *HFEs* (as a result of misdiagnoses for example). However, from my experience of PWRs, I judge that the typical key post fault actions are included and this judgement is shared by my PSA colleagues. I have raised the following AF on a future licensee (see Annex 1).

> ***AF-UKEPR-HF-04*** *– The licensee shall undertake a systematic analysis to demonstrate that all credible Type C HFEs are included in the revised Level 1 HRA.*

151 For the Level 2 PSA, three classes of action have been considered: immediate actions undertaken in the MCR; intermediate actions and long-term actions and these appear typical PWR actions. EDF and AREVA notes that the plant-specific OSSA has not been developed and hence a generic approach has been considered. They also note that aggravating errors of commission have not been addressed and that these will be considered only when the detailed task analyses have been undertaken.

> ***AF-UKEPR-HF-05*** *– The licensee shall undertake a systematic analysis to demonstrate that all credible HFEs are included in the revised Level 2 HRA.*

4.2.1.1 Assumptions Testing

152 To support the assessment of analytical completeness, I aimed to test the explicit and implicit safety-related and safety-critical assumptions. I undertook this assessment to aid my judgements on completeness. However, it relies on the presence of qualitative substantiation being available to subject the assumptions to simple HEI testing. For reasons I discuss later in Section 4.2.2 of this report, the level of substantiation expected is not available and therefore I have tabulated the assumptions and my comments on their substantiation in Annex 3 Table A3.1.

> ***AF-UKEPR-HF-06*** *– The licensee shall establish and maintain a log of current assumptions from the safety case, including consideration of those identified in Annex 3, Table A3.1. Additional assumptions should be added as they emerge from subsequent HF analysis work. All assumptions shall be substantiated as part of the forward work programme for HF.*

4.2.1.2 Conclusions

153 In general, there is a lack of evidence of adequately comprehensive processes for determining the human based safety claims and I judge that the identification of claims is not complete. I consider that there is an overreliance on operating experience and earlier safety studies and no gap analysis to demonstrate the continued applicability of claims identified for earlier evolutions of the design. There are specific features unique to the EPR and UK EPR design from that of earlier evolutions (for example the AD system) that will have an effect on the *HFEs* and potentially their risk contribution. The gaps in the model that I identified at GDA Step 3 remain.

154 However, I consider that the quantitative claims made seem reasonable; they are not exorbitant and I generally anticipate that they could be substantiated as the design

progresses. I am in agreement with my PSA colleagues that the human contribution to risk within the PSA model is adequate for overall risk estimation purposes. This stems from the explicit inclusion of post-fault operator actions within the PSA model and the implicit inclusion of human error contributions from pre-fault errors into system and equipment reliabilities and initiating event frequencies derived from operational experience. The lack of explicit consideration of pre-fault human actions and errors, is a significant deficiency for ALARP considerations, and is addressed via the assessment findings cited earlier..

4.2.2 Qualitative Substantiation of Human Based Safety Claims

4.2.2.1 Overview

155 There is no qualitative human error analysis (task analysis) presented in the November 2009 PCSR, HRA notebooks or their supporting references. Section 3 of this report details what qualitative information is available in the HRA notebooks, which I do not consider adequate evidence to support the claims made in the safety case.

156 Following significant regulatory intervention and discussion with EDF and AREVA, four task analyses were developed and presented for GDA Step 4; one Type A *HFE* and three Type C *HFEs*. For a PCSR, this is significantly below my expectations in terms of the volume of supporting analysis required. I expect all human actions to be sentenced in some manner. That is not to say that all are required to be assessed, as I do expect to see actions grouped, and bounding and risk screening arguments presented to justify the level of HF analysis required (and hence presented). Typically, I would then select a sample for my own assessment such that my judgements can be considered representative of the totality of the safety case (using targeting and proportionality principles and typically a sample size of the order that provides a 99% confidence level and a confidence interval (margin of error) of 20%). Interestingly this results in 36 actions that I would have assessed). For EDF and AREVA, this is not possible and I have assessed all four analyses. Furthermore, due to the small sample size, I am not readily able to apply firm judgements for the remainder of the safety case.

157 This lack of analysis represents a significant gap in the safety case and is my principal concern with the EDF and AREVA position for HF at the end of GDA Step 4. It is also the main focus of my GDA Issue for HF.

158 The four analyses presented are (Refs 40, 41, 42 and 43):

- Start-up of SBO Diesels, following loss of off-site power (OP_SBODG2H). (HEP = $2.1\text{x}10^{-3}$).
- Actuating the secondary cooldown following a small break Loss of Coolant Accident (LOCA) within a time window of 30 minutes (OP_FSCD_30MIN). (HEP = $4.3\text{x}10^{-2}$).
- Type A Error – Extra Boration System (EBS) Pump operation, maintenance and testing activities.
- Operator cross-connections to feed EFWS (OP_FEED_TK). (HEP = $1.0\text{x}10^{-4}$).

159 The four analyses apply a combination of Hierarchical Task Analysis (HTA), Tabular Task Analyses (TTAs) and time lines. The post-fault actions analyses also incorporate workshops and discussions with subject matter experts and detailed simulator studies..The pre fault actions assessment incorporates information from maintainers with knowledge of the activities being examined.

160 Due to the small sample size involved, and the fact that all four assessments were undertaken by the same ONR assessor, I did not formally apply or document my assessment of the four task analyses using a standard approach.

4.2.2.2 Positive Observations

161 In general, I consider the engagement of a recognised contractor and their development of this work to be a major step forward for EDF and AREVA's safety case for HF.

162 The tasks for assessment have been selected on a sound and appropriate basis. This considers the task type and how well it represents other tasks, together with consideration of the risk / safety contribution.

163 The analyses have been developed by recognised qualified and experienced HF practitioners with a sound knowledge of UK safety cases. The methods applied are generally recognised good practice and are standard approaches to this type of analysis. The analyses are clear, rigorous, offer an appropriate level of detail and are generally of a very high quality. They offer useful insight into each task and highlight the key areas for focus. The recommendations are clear and provide a valuable input to the design and forward safety analysis processes. The analyses also highlight the relative importance of the SOA and AD system and the contribution to human reliability that they are claimed to offer. I cite this as a positive aspect as it highlights a key leg of the safety argument and hence a focus for EDF and AREVA's subsequent analysis.

4.2.2.3 Assessment Observations – Specific Task Analyses.

164 I have a number of minor observations relating to the individual task analyses and these are summarised below. Additionally Annex 3 provides additional details from my Work Stream 1 assessments.

Manual Start-up of SBO Diesels following Loss of Off-Site Power within 2 hours.

165 The following omissions are noted:

- The level of workload on the operating team, particularly in the context of concurrent tasks.
- The nature of the communications demands that may exist.
- The cognitive demands on the operators and the extent to which the procedures and arrangements support them.
- The level of situation awareness that is required and that is fostered by the facilities within the MCR.
- The potential for misdiagnosis based on indications, the operation of the AD function and use of SOA procedures.
- A clear indication of the timeline for the sequence of actions, with respect to the assumptions that underpinned the time estimations and the uncertainties.

Operator Initiated Cooldown from the MCR following a small break LOCA with MHSI unavailable

- The analysis highlights that the 30 minutes rule for operator action is not achievable as the estimated time for action is at least 38 minutes.

- Insufficient consideration is given to the potential for HMI related errors and errors of navigation and there is a lack of evidence of a systematic process for identifying such errors.
- The extent to which the HMI and procedural arrangements support the staffing concept (monitoring by the OS of procedural actions by the OA, with the SS maintaining an overview) requires further analysis.
- The AD provides clear compelling indication that an initiating event has occurred and the required response. This reliance on the AD is significant and demands further explicit substantiation of its performance.
- There is insufficient analysis of how situation awareness is maintained.
- Recovery mechanisms are identified for the key human errors identified through the analysis. The reliance on these recovery mechanisms has not been adequately substantiated.

166 I have consulted with my PSA colleague and I judge that there is considerable conservatism in the overall scenario and HRA claim. The scenario should be re-examined and the claimed operator actions revised. I judge that given the insights obtained from the task analysis and the apparent conservatisms in the PSA, it is likely that an acceptable position can be reach and the claim can be substantiated, although this may require modifications to specific detailed displays or requirements for the procedures.

Maintenance of the EBS Pumps

167 My main issue with this analysis is that it was based on an equipment-level analysis and hence, does not fully consider systems level interactions. There is no analysis of concurrent tasks and activities, or of the potential for the maintenance activities to impact on adjacent systems through inadvertent actions or omissions.

168 However, I note that in light of this study, EDF and AREVA had similar conclusions about the approach and consequently intend to modify their approach to the assessment of Type A *HFEs*. I have included regulatory assessment of the revised approach into GDA Issue **GI-UKEPR-HF-01**.

EFWS Refill

- There is no consideration of automation for this task, which I judge to be an omission. I judge that automation should be considered for EFWS tank level control due to relatively fast times required for local to plant actions (and the need for actions in four separate zones) and the challenges for reliable EFWS inventory status highlighted by the analysis.
- In the absence of automation, the monitoring arrangements require strengthening and the timing and sequencing of actions requires further consideration. Consideration should also be given to partial automation of local to plant actions (such as providing MCR controls for cross-connection and tank make up).
- There is recognition of problem for the reliable long term monitoring requirement from the MCR but without a satisfactory resolution, though it is included in the HF issues register.
- There are two further omissions. Firstly the impact of the *"preferred source of make-up water via the demineralised water supply"*, which is not considered within the analysis and secondly the potential impact of the initiating event, which is an

unspecified external hazard. The first omission could alter the priority and sequencing operators undertake actions compared with that assumed in the task analysis. The lack of consideration of the impact of external hazards could hide problems of access for local to plant actions and considerable distraction for plant staff, etc. This is noted but not taken into account in the analysis.

169 The minor points I raise here on the four task analyses should be considered by EDF and AREVA at a generic level and fed forward into their forward work programme to address GDA Issue **GI-UKEPR-HF-01**. My expectations for these assessments and substantiations are commensurate with the PCSR stage of the design, and acknowledge that the HMI details and procedures are still being developed.

170 In summary, I judge that three of the tasks analysed have been partially substantiated and one is not currently substantiated. I have not recalculated the HEPs as I recognise that, as part of the revision to the HRA, the task analyses generated for GDA will be considered and applied to support the revised quantifications.

4.2.2.4 Assessment Observations – Generic

Operator Misdiagnosis

171 I recognised the implied safety importance of the AD system (and SOA) early on in my assessment of the November 2009 PCSR and the implied claim that EDF and AREVA are making on its ability to support human reliability and mitigate the potential for operator misdiagnosis. However, no holistic arguments and evidence are offered to support this claim - the task analyses presented simply argue that there is no fault diagnosis required due to the functionality of the SOA and AD system. I therefore raised RO-UKEPR-079 requiring a demonstration that the risks from operator misdiagnosis have been reduced to ALARP.

172 The key arguments presented in response to this RO are the presence of the SOA and AD system (and the fact that they do not require the operator to interpret the alarms or diagnose the events) and the staffing structure in the control room, particularly the diversity afforded by the SE (using the SICS panel and dedicated procedures rather than the SOA and AD).

173 Furthermore, it is stated that if AD fails then the operators have alternative means of performing initial orientation (and any subsequent re-orientation) by using the AD breakdown screens and paper-based support for initial diagnosis. If the PICS fails then the design provides alternative facilities on the SICS panel to perform all of the key safety tasks, including diagnosis and SICS paper-based SOA application.

174 It is further argued that recovery from operator misdiagnosis case is promoted by:

- Looping in SOA (the continual looping around the SOA procedures is designed to monitor for any plant state change irrespective of whether this has been caused by changed state due to progression of a fault transient, additional plant failures, or human error including misdiagnosis).
- The claim that the AD will alert the operator if the plant state changes, requiring exit from the current SOA and entry into a different one, means this will potentially provide a recovery route for misdiagnosis if it leads to a significant change in plant state.
- SE recovery from misdiagnosis by the OA and OS via the safety function monitoring from SICS panel. This uses diverse plant indications and relies on the SE using a paper based procedure for SOA orientation.

175 In addition, EDF and AREVA claim that they have considered the quantitative requirement by arguing that the HEPs for misdiagnosis in the HRA are judged to be conservative and that they will further consider misdiagnosis when the PSA and HRA are re-visited.

176 I accept that the SOA approach effectively removes the need for specific fault diagnosis. However, as acknowledged by EDF and AREVA, it does not remove the need for operator diagnosis at various points during emergency response. There remains a requirement to determine the appropriate initial SOA procedure to enter (initial orientation), recognise the need to move to a different SOA on changed plant state (and selection of that SOA) and undertake tactical level diagnoses within any SOA to determine the appropriate response actions (e.g. selection of the correct choice of mitigating action based on determination of precise plant status and condition).

177 At face value, I consider that the attributes described could mitigate the potential for operator misdiagnosis and will reduce their potential impact. However EDF and AREVA have not presented adequate evidence to support their claims in this area. The key omissions are:

- The consideration of failure of the AD and reliance on manual diagnosis for both initial orientation and subsequent transitions to other SOA when required.
- Tactical level diagnoses on how the design and HMI supports the claimed actions (this was highlighted as an issue by one of the task analyses).
- Operations from the SICS panel for both the diverse monitoring by the SE and performance of post-fault key safety actions by the OA and OS.

178 I have therefore included a requirement to further substantiate the claims relating to operator misdiagnosis into GDA Issue Action **GI-UKEPR-HF-01.A1** (see Annex 2)

Violation Potential

179 The November 2009 PCSR and supporting documentation does not offer any evidence relating to how the design reduces the potential for violations to ALARP. I therefore raised RO-UKEPR-80 requiring an appropriate demonstration of how the UK EPR design features mitigate the potential for violations. EDF and AREVA submitted material relating to this RO very late in the GDA Step 4 process and as a result, I have only been able to undertake a preliminary assessment of the submission. The key arguments and evidence appear to be:

- The application of operating experience to facilitate the designing out of issues that could incentivise violations.
- Application of ergonomics principles to the design resulting in systems that are simple to use, hence reducing the incentive to short cut procedures.
- The impact of violations is mitigated by the SOA and AD and the automatic logging of operator actions.
- The incorporation of violations keywords within the human error identification aspects of the task analysis programme.

180 I accept that operating experience has the potential to identify violation producing/incentivising aspects of the design but only if that experience is explicitly and directly sought. I have not been able to assess in detail the specific studies of plant operations submitted by EDF and AREVA in this regard. However, I have considered earlier studies presented as apart of the PCSR and I judge that they only partially

address the potential for violations, as their focus was on improving operational performance and reducing operator dose. Similarly, the application of ergonomics principles has the potential to reduce the violation potential but only if it is a key focus in the design process and I have no evidence to suggest that it is/was. I accept the argument that the impact of violations is mitigated by the automatic monitoring of plant state and that the task analyses processes have the potential for identify and address violation producing conditions going forward. There is further assessment to be undertaken of the material presented by EDF and AREVA in response to RO-UKEPR-80, and I have reflected this in GDA Issue Action **GI-UKEPR-HF-01.A1**.

181 In summary, EDF and AREVA have presented material relating to key areas of the HF safety case. This material provides some arguments and evidence to underpin their position but is insufficient to adequately demonstrate that the risk from operator misdiagnosis and violations is ALARP. As a result further work is required and I have incorporated this into GDA Issue Action **GI-UKEPR-HF-01.A1**.

4.2.3 Conclusions

182 My Work Stream 1 programme is the key risk informed component of my assessment strategy and the principal focus of my judgements on the adequacy of the generic November 2009 PCSR, as it is via this work that I seek assurance on the validity of the human based safety claims.

183 The EDF and AREVA position at the end of GDA Step 4 is weak with regard to my expectations for Work Stream 1. Although EDF and AREVA have a reasonable position with regard to the transparency of the claims, their work is incomplete and I am not confident in its basis (operating experience and earlier safety studies). However, there is a more significant and substantial issue regarding the lack of qualitative substantiation (analysis based evidence) provided to support the human based safety claims. I accept that the four analyses presented are generally of a high quality and reflect regulatory expectations and I consider the commencement of this work using recognised experts in the field a positive step forward. However, the overall identification and substantiation of human based safety claims is not as extensive and detailed as expected for the presentation of the HF safety case at the PCSR stage. Additionally, the empirical approach does not support an ALARP position at the end of GDA Step 4.

184 The GDA Issue that I have raised is to reflect that the gap is substantial and there is a significant volume of analysis to be undertaken before I can consider closing the GDA issue.

4.3 Work Stream 2: Generic Human Reliability Assessment – Assessment

185 At the end of GDA Step 3, both PSA colleagues and I reported queries regarding the application of the HRA methods used for the UK EPR, particularly the application of different HRA methods for the Levels 1 and 2 PSA (Refs 6 and 19). My work for GDA Step 3 on HRA focused on understanding the human based safety claims and I concluded that the model had included post-fault operator actions but that the consideration of Type A *HFEs* was limited. Overall, I concluded that EDF and AREVA have a good understanding of the contribution of human actions to safety. I also noted in GDA Step 3 that I would consider the treatment of misdiagnosis and dependency further during my GDA Step 4 assessment.

186 The assessments that I have undertaken relating to the HRA model in GDA Step 4 have not altered my opinion with respect to the broad conclusions that I reached at the end of GDA Step 3. However, I have looked in significantly more detail at specific aspects of the HRA and this is explored below.

187 My judgement on the quality of the HRA aligns with that of my PSA colleague, at the end of GDA Step 4, that there are omissions in the HRA model and that some claims will need to be revised in the light of detailed analyses being undertaken. This results in the requirement for a revision as the risk assessment for the UK EPR progresses beyond the PCSR stage. This requirement is cited as an Assessment Finding (AF-UKEPR-HF-01); as my judgement is that the integrity of the HRA risk model will not have a significant impact on the design of the UK EPR or the overall acceptability of the PSA.

4.3.1 Relevance of Extant HRA Techniques for the Assessment of Modern Control Room Task Environments

188 I note the application of the ASEP (Ref. 26) and SPAR-H (Ref. 27) methodologies to the UK EPR HRA. Both of these methods use data taken from, or based on, (the) Technique for Human Error Rate Prediction (THERP) data. THERP is a recognised ‘first generation’ HRA method first published in 1982, in the era of second generation NPPs with traditional hard wired control room environments. The THERP manual (Ref. 13) explicitly highlights that *“the handbook does not provide estimated HEPs related to the use of new display and control technology that is computer based”*. THERP is applied widely and generally accepted for use in UK NPP risk assessment. However, the levels of automation and computerised control and instrumentation apparent in the UK EPR design calls into question the applicability of THERP data to modern NPP HRA. I therefore commissioned research into (derived) HEP data from contemporary literature and this is reported below, together with a discussion on the impact or otherwise on THERP data.

189 There were 85 human error data points which were obtained from 35 referenced sources. All of these sources are concerned with human computer interaction and are considered relevant to process control. The error data came from tasks of two broad types. Firstly, errors are reported from holistic tasks (tasks that are complete and described at a level that can be related directly to tasks performed for process control or emergency response in the nuclear industry). The second and predominant type of study found in the literature has been narrower in scope. These concern particular kinds of subtasks or interface objects that would comprise part of a process control or monitoring task.

Holistic Tasks Data

190 The detail of the four experimental studies relating to holistic tasks is reported in Annex 5 and the error probabilities associated with them reported in Table 9 below:

Table 9: Holistic Task Experimental Studies

Holistic Task	Reported Error Probability	Comment
NPP start-up with automated support	$2.0\text{x}10^{-3}$	Team error probability per functional interaction

Table 9: Holistic Task Experimental Studies

Holistic Task	Reported Error Probability	Comment
Collaborative virtual team task errors	$2.0\text{x}10^{-3}$ (derived)	Team error probability
Decisions on tabulated parameters	$5.0\text{x}10^{-3}$	Individual error probability
Knowledge of finite state automation	$9.0\text{x}10^{-3}$	Individual error probability

Implications of Holistic Data for THERP

191 The start-up task in the first study (Ref. 22) is routine and therefore no diagnosis would be necessary. On the basis that the tasks are supported by automated procedures and interfaces, they could be considered amenable to assessment as THERP rule-based actions. Clearly, the probabilities that will emerge in an experimental study of this kind are those of the dominant errors. The probabilities reported in this first study are within the range for the reading and recording of quantitative displays and the check reading of qualitative displays given within THERP Tables 20–10 and 20–11.

192 It is also consistent with the higher probabilities offered for control selection in use in THERP Table 20–12. However, THERP offers the possibility to apply recovery and this would result in assessments that were considerably more optimistic than those derived within the study. Therefore, my provisional conclusion is that the application of THERP estimates to HCI based upon this one study, are likely to be optimistic.

193 In stating that there is potential for optimism in a THERP assessment relative to the reported data, consideration must also be given to whether the study is offering pessimistic estimates relative to ‘real life’. The preparation of subjects for the study and their level of expertise, suggests that better performance might be achieved with longer training. However, countering that argument for improved reliability, it should be noted that the team set up was reactor operator, assistant reactor operator and supervisor. The supervisor had no additional tasks to do other than monitoring the performance of the two operators. That is, the supervisor was more lightly loaded than reality. Overall therefore, it may be concluded that the application of THERP to HCI tasks of this kind is likely to result in an optimistic estimate of human reliability. My provisional conclusion is that THERP offers a baseline assessment of error probability that is likely to be optimistic.

194 The second study (Ref. 23) on collaborative working covers many diverse and un-described tasks and therefore it is difficult to compare these unspecified tasks with nuclear process control tasks. Nevertheless, it is interesting because it suggests some level of performance for teams distributed across space and time. The character of the tasks may well be similar to those undertaken when a control room team interacts with a remotely located Emergency Control Centre.

195 The third task (Ref. 24) is closely comparable to the processing of alarms and computer-generated lists, as opposed to the form of alarm annunciators assumed within THERP, i.e. spatial arrays of trans-illuminated tiles. It is interesting to identify the corresponding alarm error probability within THERP. The THERP Table 20-23 suggests that the

probability of failing to respond to any one of five alarms is 3.0×10^{-3}. The number of alarms being processed within the tasks performed throughout the study was 15. This suggests that the THERP annunciator response model may be conservative when applied to a modern computer generated alarm system with good alarm classification and on-screen prioritisation coding. The study was also undertaken with subjects performing under considerable time pressure (three minutes per session) and so the simulation can be considered close to real world conditions. It should be noted that the prioritisation attached to alarms meant that any additional learning of alarm 'meaning' would probably not have improved reliability much beyond that seen in the study.

196 The fourth study (Ref. 25) concerns how well individuals, who must interact with automation such as protection systems or on board flight systems, understand their programmatic rules and how such systems operate. Where the operators have been given training on the system automation function, it is frequently experienced, and has a strong attentional focus, their knowledge and understanding of that programmatic behaviour has an error rate of 9.0×10^{-2}. However, if there has been no training on the automation function, it has not been frequently experienced and also suffers from a weak attentional focus, then the error rate is as high as 9.0×10^{-1}. This shows that there is an important re-allocation of function issue and an overall human reliability issue if automated control reverts to manual operation under conditions of failure. This may be important, not only in terms of automation applied to process control, but also to automation which supports and guides process control task performance in the guise of semi-automated procedures or automated interface configuration and displays selection. This 'cliff edge' effect is important and is not addressed in THERP.

Object Level Tasks Data and Implications for THERP

197 Essentially, the studies of human interactions at the object level produce broadly similar results and therefore the studies are not described separately but in overall groupings. A narrative description of these studies is presented in Annex 4. Table 10 presents the derived data and provides a comparison with the closest available THERP data point. The derived data represents the best available (i.e. most optimistic) human reliability data contained within the object level studies identified in the literature. Therefore, this table is the most generous interpretation of the suggested reliabilities that might be obtained when conditions are favourable for the kinds of objects studied. I have also presented summary statistics at the end of Table 10. A log-normal distribution has been assumed and the mean of the assumed log-normal distribution has been calculated by taking the average of the log (unreliability) for all included data points. The fifth and 95th percentile points have been obtained from the same log values of the data. The summary statistics at the end of Table 10 clearly show that the HEPs obtained for the studied objects are higher than those which would apply for THERP even at the better end of the range.

Table 10: Object Level Task Experimental Studies

Experimental Effect	Derived Experimental Data HEP	THERP closest 'equivalent' HEP
Parallax effects of process screen parameter reading no parallax	1.7×10^{-2}	No direct equivalent. Table 20-11, items 1 and 2 provide the most optimistic HEPs for the check reading of displays at 1.0×10^{-3}.

Table 10: Object Level Task Experimental Studies

Experimental Effect	Derived Experimental Data HEP	THERP closest 'equivalent' HEP
Icon selection--double click	5.0x10^{-2}	No direct equivalent. Tables 20-9 and 20-12 items 2, 3 and 4 provide HEPs for errors selecting controls and displays. The lowest HEP provided is 5.0x10^{-4}.
Label icon and help	4.2x10^{-2}	No direct equivalent. Tables 20-9 and 20-12 items 2, 3 and 4 provide HEPs for errors selecting controls and displays. The lowest HEP provided is 5.0x10^{-4}.
Selection of eliminated/ gapped menu items with feedback but no error recovery	7.4x10^{-3}	No direct equivalent. Tables 20-9 and 20-12 items 2, 3 and 4 provide HEPs for errors selecting controls and displays. The lowest HEP provided is 5.0x10^{-4}.
Shallow wide menu	3.0x10^{-2}	No direct equivalent. Tables 20-9 and 20-12 items 2, 3 and 4 provide HEPs for errors selecting controls and displays. The lowest HEP provided is 5.0x10^{-4}.
Modify with drag of function to object	2.8x10^{-2}	No THERP equivalent
Random soft keyboard	5.9x10^{-3}	No THERP equivalent
Non perseverated ("stuttered") sequential non-software modified keying, disabled and non disabled users	2.5x10^{-3}	No THERP equivalent
Data entry from memory chunked in 2's 1-3 digits	5.0x10^{-2}	Table 20-10 item 8 suggests a 'Negligible' HEP
Interlock knowledge errors PER ROW	3.0x10^{-3}	No THERP equivalent
Database Boolean searches – young subjects	1.3x10^{-2}	No THERP equivalent
Info retrieval -linear structure – young subjects	4.0x10^{-2}	No THERP equivalent
Knowledge of finite state automation with frequent experience in use and strong attentional focus	9.0x10^{-2}	No THERP equivalent
Computer assisted readiness checks	5.0x10^{-1}	No THERP equivalent

Table 10: Object Level Task Experimental Studies

Experimental Effect	Derived Experimental Data HEP	THERP closest 'equivalent' HEP
Diagnostic decision making performance no time pressure	$3.1x10^{-1}$	Table 20-1, item 6, $1.0x10^{-4}$
Diagnostic decision making expert rule system support	$5.0x10^{-1}$	No THERP equivalent
Automatically supported diagnostic decision making short tree OR heuristics	$1.8x10^{-1}$	No THERP equivalent
Local task language – simple	$3.0x10^{-1}$	No THERP equivalent
Virtual team collaborative error	$2.0x10^{-1}$	Table 20-02, most optimistic HEP $2.5x10^{-2}$
Self-recognition of handwriting for logon authentication with recovery	$9.4x10^{-3}$	No direct equivalent. Tables 20-9 and 20-12 items 2, 3 and 4 provide HEPs for errors selecting controls and displays which are tasks of recognition. The lowest HEP provided is $5.0x10^{-4}$.
95th percentile	$5.0x10^{-1}$	$1.6x10^{-2}$
Lognormal distribution mean	$2.9x10^{-2}$	$4.0x10^{-3}$
Fifth percentile	$2.5x10^{-3}$	$2.4x10^{-4}$

198 I recognise that these levels of unreliability may not necessarily result in unfavourable consequences. It could be argued that unsuccessful interactions with menus, inappropriate 'mousing', breakdowns of keyboard entry and icon selection are all amenable to self recovery. This raises the prospect that experimental studies which measure error without feedback of the error and opportunity of recovery are unduly conservative (i.e. pessimistic). Further theoretical discussion in this regard is offered in Annex 5.

199 Furthermore, it is not unusual for HF experimental studies to obtain statistically significant differences that are of little significance in terms of human reliability. In studying the literature, the magnitude of experimental effects has also been examined and reported in Annex 5.

200 In conclusion, the 'data' that I have derived relating to contemporary human computer interfaces suggests a higher level of human unreliability when compared to human interactions with traditional controls and displays. However, I recognise that this data is not readily available, verified or validated in any scientific manner nor is it readily assembled into recognised and contemporary HRA methodology. I therefore note that traditional first generation HRA methods (such as THERP) may not be applicable for HRA of modern NPPs. This finding is equally relevant to methods such as ASEP and SPAR-H that incorporate, or are based on, THERP data. I suggest that prospective licensee

organisations consider the applicability of extant HRA methods to the UK EPR HRA revision and note my regulatory expectations in this regard as cited in SAP EHF.10 (paragraph 390: *"The selection and application of probability data for human errors should be……..justified and its relevance for the task and context demonstrated"*) and TAG T/AST/063 (Ref. 7) on HRA.

> **AF-UKEPR-HF-07 –** *The licensee shall review available HRA methods for the proposed UK EPR HRA revision, in the light of the digital nature of operator interfaces. The choice of HRA method shall be justified as appropriate in line with ND TAG T/AST/063.*

4.3.2 Application of the ASEP and SPAR-H HRA Methods and Treatment of Diagnosis in HRA

201 The three aims of this aspect of my assessment were to:

- Examine the generic application of the ASEP and SPAR-H methods to the HRAs that EDF and AREVA have presented in the Level 1 and Level 2 PSA.
- Consider the implications of applying ASEP to the Level 1 PSA and SPAR-H to the Level 2 HRAs.
- Examine the EDF and AREVA treatment of diagnoses in HRA.

4.3.2.1 Level 1 PSA General Application of the ASEP Method

EDF and AREVA Modelling Content Overview

202 EDF and AREVA have used ASEP for the HRA in the Level 1 PSA for pre-fault and post-fault actions. The application of the ASEP method is described in Section 3.5 of Subchapter 15.1 of the PCSR (Ref. 17) and further details are given in the substantiation and identification document (Ref. 28).

203 The approach described within the submitted documentation broadly follows the architecture of the process given within the ASEP manual, with detailed differences in recovery that I discuss below.

Level 1 Pre-initiating Event Actions

204 The treatment of pre-initiating fault errors broadly follows the architecture of the approach given by ASEP. The basic human error probability of $3.0\text{x}10^{-2}$ is identical to that given within ASEP. ASEP allows for recovery of pre-accident task errors as a function of combinations of component status, second person checks, status verification checks and per-shift or daily checks. The document identifying and substantiating key claims on operator reliability (Ref. 28) states the approach that has been followed is equivalent or more conservative to that given in the ASEP method. The original ASEP values and descriptors are compared with those chosen by EDF and AREVA in Table 11 below. Probabilities are shown in parentheses. As the Key HRA claims document (Ref. 28) states that *"In a further conservatism only a single recovery factor was applied to the basic HEP even where several different factors favouring recovery would be present"*. . The most optimistic value of recovery probability has been chosen when more than one ASEP category could be judged equivalent to account for the fact that multiple factors would be present.

Table 11: ASEP to EDF AREVA Pre-initiator Recovery Comparisons

ASEP Descriptor	RP Equivalent	Notes
The existence of "compelling signals" ($1.0\text{x}10^{-5}$)	Category 1 alarm (visual and sound warning) ($1.0\text{x}10^{-3}$) Alarm of category other than 1 ($1.0\text{x}10^{-1}$)	
Recovery by post maintenance or post calibration test ($1.0\text{x}10^{-2}$)	Anomaly detectable by checks planned during standard state changes ($1.0\text{x}10^{-3}$) Commissioning and requalification enabling the anomaly in question to be effectively detected ($1.0\text{x}10^{-2}$) Periodic test ($1.0\text{x}10^{-2}$)	This could have been assigned to the next ASEP category down at $1.0\text{x}10^{-1}$
A separate check of component status at a different time and place ($1.0\text{ x}10^{-1}$)	Indication of position in control room ($1.0\text{x}10^{-1}$)	This interpretation is only applicable if the realignment is undertaken local-to-plant
A shift or daily check of component status using a written list with checkboxes ($1.0\text{x}10^{-1}$)	Large change in the value of the parameter recorded during each shift ($1.0\text{x}10^{-2}$)	
Supervisory sign off (claimed only in so far as it ensures that the required task was initiated) ($1.0\text{x}10^{-1}$).		
No ASEP equivalent	Key lock with supervision of key ($1.0\text{x}10^{-3}$)	

205 These comparisons highlight that there are three categories of recovery factors that I consider to be more optimistic than the original ASEP values:

- Anomaly detectable by checks planned during standard state changes.
- Large change in the value of the parameter recorded during each shift.
- Key lock with supervision of key.

206 I therefore conclude that the assertion of the approach being more conservative than ASEP is not always correct. However, it is important to note that the ASEP recovery cases provide factors of recovery numerically ranging from $1.5\text{x}10^{-1}$ to $1.0\text{x}10^{-5}$. Moreover, out of the nine permissible combinations of ASEP cases that exist, six are below $1.0\text{x}10^{-2}$. Therefore, in numerical terms the distribution of EDF and AREVA's recovery factors is over a narrower and more pessimistic probability range than those provided by the original ASEP method. However, it is worth examining the three cases that appear to be more optimistic than ASEP.

207 A standard state change is a frequent occurrence. However, more detailed methods such as THERP that offer recovery failure probabilities would not propose such a high recovery value as that put forward here. In effect, this claim on recovery at 1.0x10^{-3} is as good as making the check an entirely independent task. Therefore, I consider this generic probability of recovery considerably over optimistic.

208 The ASEP claim on a routine check provides for one order of magnitude improvement, i.e. an error rate of 1.0x10^{-1}. However, EDF and AREVA have elaborated on this by including the additional requirement that the value of the parameter should be both recorded and that the change in the value should be large. Although the method of record and the characteristics of a large change have not been precisely defined, it is reasonable to suppose that a parameter recorded, e.g. during shift change and changed by a significant amount could be credibly claimed at two orders of magnitude. However, whilst I consider this may be a realistic recovery claim, I do consider that a large change must be defined as one which is well beyond the observer's expectations.

209 There have been persistent debates over the years about the benefit of keys for human reliability. Keys that are unique to each key switch have a serious potential to disrupt emergency actions that must be undertaken quickly and efficiently, as the wrong key can be issued. This can either prevent the correct action being taken or induce the wrong action. In summary, key selection merely transfers the error from switch selection to key selection, although standard keys applicable to multiple switches do not constitute a barrier to incorrect switch operation. Repeated nuclear incidents have shown that standard keys must be used to avoid key confusion during maintenance and the blocking of actions in emergency operation. Therefore, a key switch with standard keys does not constitute any form of defence either against a selection of the incorrect control or the inappropriate operation of the correctly selected control. It only prevents operation by a person not holding a standard key. Unfortunately, nuclear operational history also illustrates that the manifest and clear obstruction engendered by keys and the implied lack of trust between supervisors or managers and operational staff, results in keys tending to be issued for uncontrolled use, usually on the entirely rational basis that those who will use the keys are suitably qualified and experienced to do so. Either that, or keys are always left in locks. Therefore, I doubt the claimed benefits of key locks when applied to solitary key switches.

210 However, it should be noted that the above remarks do not apply to robustly engineered key-operated interlocks that are operated as part of a key exchange sequence. In this case, the reliability should be bounded by the reliability of the interlock scheme, or if the scheme is complex, the reliability of the human in understanding the correct operational sequencing and branching of that scheme. In the case of understanding, this reliability is considerably less than that which would be achieved in numerical terms by the application of the recovery factor of 1.0x10^{-3} offered by EDF and AREVA. At the very best, a key issued by a supervisor can only prevent an action occurring at the wrong time. It cannot, on a key switch, ensure that the correct action happens at the right time. Therefore, it does not constitute a means for recovery.

211 I conclude that the EDF and AREVA modifications to the ASEP method for pre-accident task recovery, either by anomaly detection or supervised key lock operation, have resulted in the application of optimistic recovery factors in the case of standard state changes and key switch operation.

> ***AF-UKEPR-HF-08 –*** *The licensee shall justify the HEP values applied for pre-accident task recovery in the light of comments made in the GDA Step 4 HF report, as part of the HRA revision*.

Level 1 Initiating Event Actions

212 This section concerns human errors that initiate an incident (Type B errors). Reference 28, which substantiates key claims on operator reliability, states "*the frequencies of events with the potential for initiation of a core damage fault sequence are assessed in Reference [4, Chapter 2] on the basis of several hundred reactor years of accumulated French and worldwide PWR operating experience*".

213 I commend the application of data rather than a synthetic human reliability assessment method for initiating events. However, such data cannot be taken at face value and typically requires some post-processing in order to provide accurate estimates of human error probability.

214 There is insufficient substantiation information presented by EDF and AREVA to understand how the data for these *HFE*s have been processed. Therefore, it is not possible to determine whether the assessed frequencies for error are likely to be optimistic or not. However, there are three principal factors which render such data optimistic when applied in its raw form: masking, underreporting and dilution.

215 I conclude that insufficient information has been presented to understand whether the potential for a substantial underestimation of human error in initiating events has been compensated for within the data that has been applied.

> ***AF-UKEPR-HF-09 –*** *The licensee shall provide information on how the raw data applied to Type B HFE quantifications has been processed, as part of the HRA revision.*

Level 1 PSA Modelling of Post-fault Actions

216 A generic table for ASEP probabilities (Section 15.1.3 Table 4 in Ref. 17) provides the structure for all claims on human reliability. Each claim takes the following form:

P(Overall error) = P(diagnostic error) + (1 – diagnostic error) x P(Action error) x P(Action recovery error)

217 The diagnostic error probability is derived by first calculating the time available for diagnosis. This is obtained by taking the shortest credible transient timescales and subtracting five minutes. The five minutes represents a standard time assumed for actions, thereby leaving all the remaining time available for diagnosis. The diagnostic probability is then derived from ASEP Table 7-2, which is in turn a direct copy of THERP Table 20-1. This provides an assessed screening (i.e. nominally conservative) probability of diagnostic error.

218 The probability of action error is derived based upon moderate stress ($5.0x10^{-2}$) or high stress ($2.5x10^{-1}$). These values are taken directly from ASEP. Moderate stress is applied for all actions except Primary Bleed and Feed, where high stress is considered applicable.

219 The ASEP method prescribes that post-fault actions performed under moderately high stress should have an assigned error probability of $2.0x10^{-2}$ in a screening assessment. A screening assessment is one where the analyst is not yet confident about the applicable factors. Section 3.5.2.3 of Subchapter 15.1 (Ref. 17) prescribes the same probability. Similarly, a probability of $2.5x10^{-1}$ for tasks performed under extremely high stress is prescribed by ASEP and in (Ref. 17).

220 ASEP offers a more optimistic value of $1.0x10^{-2}$ than either of the above, within the set of screening data. This is for skill-based actions committed to memory. However, this has not been included within the method applied by EDF and AREVA.

221 I conclude that conservative values have been applied using the ASEP method for application to Level 1 post-fault actions, as screening, rather than nominal values, have been applied

Error Recovery for Post-fault Actions

222 ASEP does not include an allowance for action error recovery in the Section 7 post-fault screening tables. However, recovery by alarms and independent checking is included within the nominal assessment tables provided in Section 8. However, neither the ASEP Section 7 nor 8 approaches are applied by EDF and AREVA who have offered an alternative approach where recovery is based upon the time available. This is presented in PCSR Section 3.5.2.4 of subchapter 15.1. Essentially, within the MCR if the time available exceeds 30 minutes, recovery is asserted to occur on seven in 10 occasions. If the time available exceeds 60 minutes, then recovery will occur on seven in 100 occasions. However, if action is required outside of the MCR and more than 60 minutes is available, then recovery will succeed on 20 in 100 occasions. No justification for these assertions is offered and I cannot find any relationship between this approach and data in, say, THERP or any other human reliability assessment method that is more detailed than ASEP.

223 I also note that, despite the fact that all actions are assumed to take five minutes, recovery of failed actions is assumed possible as a function of the total transient time available, including the time assigned and “used up” for the derivation of diagnostic error probability. This is not an internally logical or consistent approach to the use of time, as the same time is being claimed for the purposes of maximising diagnostic time available to minimise assessed diagnostic error probability, and maximising action error recovery time, to the benefit of action error recovery probability.

224 I conclude that despite the potentially conservative approach to human error probability estimation via the adoption of the ASEP screening tables, this conservatism is negated by the unsubstantiated application of numerical recovery factors, which are not justified by data and which appear to be qualitatively illogical.

> ***AF-UKEPR-HF-10*** *– The licensee shall justify the quantitative modelling of error recovery as part of the HRA revision.*

4.3.3 Level 1 PSA Modelling of Post-fault Diagnosis

225 There are two distinct aspects that I have considered in the application of ASEP to the EPR PSA. The first is whether the ASEP method has been applied as intended by its originators and, if not, whether the resulting assessments are more or less conservative (pessimistic) as a result of any changes in the application of the method that may have been made. The second aspect I have considered is the qualitative phenomena such as tasks, error producing mechanisms and performance shaping factors that have been recognised in the application of the method as reported.

4.3.3.1 Application of ASEP Method

226 As stated earlier, the diagnostic error probability is derived by first calculating the time available for diagnosis. This is obtained by taking the shortest credible transient timescales and subtracting five minutes. The five minutes represents a standard assumed time for actions thereby leaving all the remaining time available to diagnosis. The diagnostic probability is then derived from ASEP Table 7-2, which is in turn a direct

replication of THERP Table 20-1. This gives an assessed screening (i.e. nominally conservative) probability of diagnostic error.

227 The probability of action error is derived based upon moderate stress ($5.0x10^{-2}$) or high stress ($2.5x10^{-1}$). These values are taken directly from ASEP. Moderate stress is used for all actions except Primary Bleed and Feed, where high stress is considered applicable.

228 I have already discussed in Section 4.3.1 that it is very likely that the estimates of diagnostic error probability are optimistic. It should also be noted that within the bounds of the method, it has been universally assumed that the duration of post fault actions following diagnosis will take no longer than five minutes. Accordingly, this extends the time available for diagnosis and improves the corresponding reliability within the ASEP method. It seems most unlikely that a universal nominal time for action of five minutes will apply in practice. Therefore, even within the bounds of the method and assuming it to be valid, the calculations of diagnostic error probability will be optimistic. Overall, I conclude that the derivation of diagnostic error probability is optimistic within the bounds of the ASEP method and that, relative to published data, the method itself is likely to be optimistic. Therefore, on both counts estimates of diagnostic error are likely to be optimistic.

> ***AF-UKEPR-HF-11 –*** *The licensee shall justify the approach for the HRA modelling of diagnostic errors when revising the HRA.*

4.3.3.2 Applicability of Modelling

229 Post-fault diagnosis is intended to be through the use of the computer supported AD system. However, as this is a software-based system, it must have probabilities for failure modes and complete system failures that are of the same order or possibly even of lower reliability than for human diagnostic error probabilities. As a result, it will be necessary in practice to make a claim on the backup panel, alarms and manual procedures. That is upon the use of the SICS. This is currently not reflected in any way within the case (HRA) that is presented. This is a significant omission in the overall safety case and has been recognised in the Work Stream 1 assessment of qualitative substantiation of human based safety actions assessment. Any claims required relating to the SICS panel will require substantiating as part of GDA Issue **GI-UKEPR-HF-01.A1**.

4.3.4 Level 2 PSA General Application of the SPAR-H Method

230 The Level 2 supporting human reliability analysis is contained in Ref. 30. In contrast to the Level 1 PSA, the SPAR-H method has been used. The comparison of ASEP and SPAR-H is outlined in Sections 4.3.5.1 and 4.3.5.2 for post-fault diagnostic and corrective actions respectively. This work results in my judgement that the SPAR-H method will lead to a more optimistic assessment than ASEP as originally conceived.

4.3.4.1 Application of the SPAR-H Method

231 Inspection of the Level 2 HRA documentation (Ref. 30) and in particular Tables 9 and 10 for non-OSSA and OSSA actions respectively, suggests that SPAR-H has generally been applied in an appropriate manner.

232 However, I consider that there has been one notable departure from the typical basis for the application of SPAR-H. This is a modification to match the OSSA strategy roles,

namely the control room crew, the TSC and the emergency director and the interactions between them. SPAR-H was developed to consider control room crew responses using Emergency Operating Procedures (EOP) rather than for the OSSA based response. This modification of SPAR-H has not been justified. Additionally, I judge that the event tree (Figure 3 of Ref. 30) used to determine the OSSA response within the Level 2 has not been adequately justified.

> ***AF-UKEPR-HF-12 –*** *The licensee shall justify the HRA method applied to the revised Level 2 PSA, and clearly highlight any deviation from its typical and expected application*.

233 I now consider the detailed aspects of the numerical application of SPAR-H within the HRA for the Level 2 PSA.

234 SPAR-H suggests that a base case should be confined to the first three performance shaping factors (as used in the comparative examples provided earlier). However, inspection of Tables 9 and 10 of (Ref. 30) shows that all eight performance shaping factors have been made available for application hence exceeding the prescription of the method at the design stage. However, three of the eight have always been set at the nominal level (i.e. at Unity), these are:

- HMI.
- Fitness for duty.
- Work processes.

235 Three of the other performance shaping factors have been used to degrade estimates of human reliability:

- Stress.
- Complexity.
- Procedures.

236 Two PSFs have been used to improve estimates of human reliability:

- Timing.
- Training.

237 No factors have been used either positively or negatively in different cases.

238 In accordance with the method, timing has sometimes improved estimates of human reliability where the time available for diagnosis is between one and two times the nominal time and greater than 30 minutes (x $1.0\text{x}10^{-1}$), or greater than twice the nominal time and greater than 30 minutes (x $1.0\text{x}10^{-2}$). For reliability improvement in actions, time available has sometimes been assessed as greater than five times (x $1.0\text{x}10^{-1}$) or 50 times the time required (x $1.0\text{x}10^{-2}$). Training has been assessed as high in a number of instances giving an improvement of x $5.0\text{x}10^{-1}$.

4.3.5 Implications of Applying ASEP to the Level 1 PSA and SPAR-H to the Level 2 HRAs

239 To understand the potential implications of applying differing HRA methods between the Level 1 and Level 2 PSA, I reviewed ASEP and SPAR-H to both examine the methods and to determine the likely implications arising from their application to the PSA.

4.3.5.1 Comparison of ASEP with SPAR-H for Post-fault Diagnosis

240 Both ASEP and SPAR-H apply the mathematical treatment of human dependency that is put forward in THERP. Therefore, in mathematical terms the same dependency outcomes could be expected. As the methods are formulated on an entirely different basis, the only useful way to undertake a comparison is to consider their application in some benchmark scenarios, which I have undertaken below. In undertaking the comparisons, I focused on the first three PSFs within SPAR-H, which are used for a base case, as these are appropriate for a new plant that is yet to be built. These are: time available, stress and stressors and complexity. The method supposes that the other factors cannot be known until a plant is working. These are: experience/training, procedures, ergonomics/HMI, fitness for duty and work processes.

241 In these comparisons, reference is made to the third performance shaping factor within SPAR-H which is termed “complexity”. Figure 2 below is taken from the method and illustrates the SPAR-H meaning of complexity.

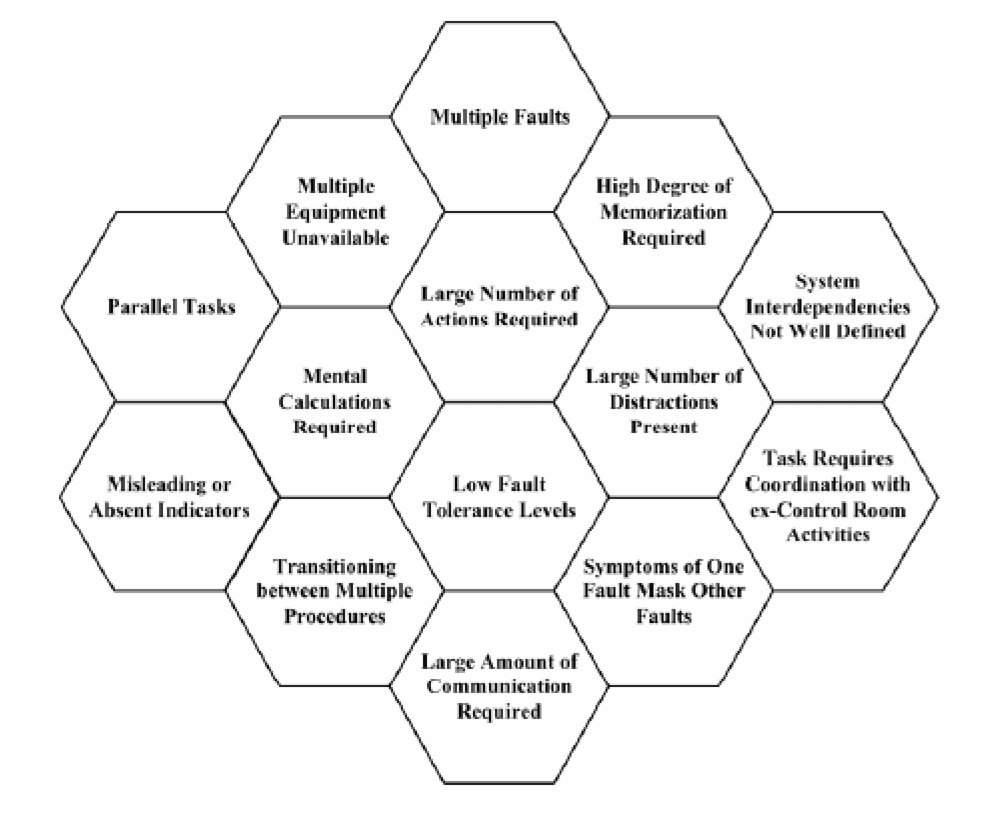

Multiple Faults
Multiple Equipment Unavailable
High Degree of Memorization Required
Parallel Tasks
Large Number of Actions Required
System Interdependencies Not Well Defined
Mental Calculations Required
Large Number of Distractions Present
Misleading or Absent Indicators
Low Fault Tolerance Levels
Task Requires Coordination with ex-Control Room Activities
Transitioning between Multiple Procedures
Symptoms of One Fault Mask Other Faults
Large Amount of Communication Required

Figure 2: SPAR-H’s Figure 2-3 Factors contributing to complexity

242 Each scenario is briefly documented and then assessed. The minimum of comparative commentary is given in each assessment and comparisons are drawn in a separate subsection at the end. As both methods draw a distinction between diagnostic error and action error, assessments are made according to the scheme.

243 It should be noted that the comparisons that have been made use the screening ASEP assessment approach throughout, as EDF and AREVA have applied the ASEP screening method. The ASEP screening approach, which is more pessimistic, will give greater differences than the nominal. The nominal ASEP central estimate is given in parentheses.

Comparative Scenario 1: Very Rapid Diagnosis

244 For the purposes of making this comparison, it is assumed that the diagnosis needs to be made with no support beyond conventional displays and alarms, i.e. there is no automated diagnostic support.

245 The transient timescales for the fault in question are about 20 minutes. The single electrical system fault is easily identifiable as significant to nuclear safety and is to be diagnosed by the control room crew without local to plant support. The fault is covered by initial training and will be well represented by the alarm system but will cause a cascade of alarm indications to occur. The time to make the diagnosis following the onset of fault annunciation is estimated to be 10 minutes. The time for action will be between five and seven minutes. Considering the combined time of diagnosis and action, the time available overall is barely adequate.

246 ASEP provides a diagnostic error reliability of $5.0\text{x}10^{-1}$ ($1.0\text{x}10^{-1}$) with an error factor of five giving a probability range from one to $1.0\text{x}10^{-1}$.

247 The SPAR-H model offers a diagnostic error probability of $1.0\text{x}10^{-2}$. As the nominal time available to perform the task exists, this does not change the probability. However, the overall short timescales and the safety significant (but not safety-critical) nature of the fault can be argued to lead to high stress (x2). Considering the factors contributing to the task complexity, it is arguable that a large amount of communication may be required to tease out the actual fault from the number of alarm indications occurring. Accordingly, the diagnosis can be argued to be moderately complex (x2). Therefore, the overall error is estimated at $4.0\text{x}10^{-2}$. The SPAR-H estimate is, however, about an order of magnitude more optimistic than ASEP.

Comparative Scenario 2: Rapid Diagnosis

248 For the purposes of making a comparison, I have taken the same scenario as above but the required task time occupied in diagnosis is now increased to 15 minutes. This means the entire diagnostic and action task may just be credible within the time available or there may be an overall shortfall of two minutes, assuming there is no pause between diagnosis and execution of action (e.g. to obtain an appropriate procedure).

249 In this case, the ASEP estimate will remain the same as before: a reliability of $5.0\text{x}10^{-1}$ ($1.0\text{x}10^{-1}$) with an error factor of five giving a probability range from one to $1.0\text{x}10^{-1}$.

250 SPAR-H will now invoke an additional performance shaping factor of barely adequate available time, which places an error multiplier of 10 into the equation. As the stress due to time shortages is already accounted for by the other two performance shaping factors, they are left as they are. As there are now three performance shaping factors present, all of which are negative, it becomes necessary to use the prescribed SPAR-H calculation adjustment based upon odds given within the method.

Nominal HEP = 0.01, PSFcomposite[5] = 10 x 2 x 2 = 40

HEP = Nominal HEP x PSFcomposite / (Nominal HEP x (PSFcomposite - 1) +1)

HEP = 0.01 x 40/(0.01x(39) + 1) = 0.4/1.39 = $2.0\text{x}10^{-1}$.

251 It can be seen that the SPAR-H estimate is now sensitive to the tight time constraint and is consistent with ASEP within a factor of 2.5. If the task time exceeds the available time

[5] ‘PSFcomposite’ represents the combination of PSFs applicable to the error.

the actual error probability could equate to one. This depends on any continuing usefulness of actions beyond the allotted transient timescale.

Comparative Scenario 3: Longer Diagnostic Timescales

252 A fault has an assessed diagnostic time of 10 to 15 minutes. There is no requirement to achieve a diagnosis before 30 minutes and actions may be taken within the first hour following the onset of the fault.

253 ASEP provides a nominal diagnostic error probability of $1.0\text{x}10^{-2}$ ($1.0\text{x}10^{-3}$) with an error factor of 10 giving a probability range of $1.0\text{x}10^{-2}$ to $1.0\text{x}10^{-4}$.

254 The SPAR-H nominal diagnostic probability can, in principle, be modified by performance shaping factors. Although there is extra time available to make diagnosis of approximately two times the nominal, the diagnostic time remains less than 30 minutes and therefore the method precludes the use of the expansive time performance shaping factor to enhance the reliability estimate. In this circumstance, stress can still be deemed to be high (as per scenario 2), as can complexity. Therefore, the nominal error probability is $4.0\text{x}10^{-2}$. This is within a factor of four of ASEP.

Comparative Scenario 4: Diagnostic Time Greater Than 30 Minutes

255 This scenario is identical to the previous one except that an hour is now available to make a diagnosis but the actual time taken to make a diagnosis is unlikely to be more than the 15 to 20 minutes previously cited.

256 For ASEP, in this instance, it becomes debatable whether the diagnostic probability should be taken as that which relates to the diagnostic task execution time or to the time available. Strictly, the method prescribes that the reliability is a function of the time available, hence giving a more favourable estimate. If the diagnostic task execution time is taken, then the nominal diagnostic error probability is $1.0\text{x}10^{-2}$ ($1.0\text{x}10^{-3}$) but if the method is strictly followed and the available time is used, then the estimate is $1.0\text{x}10^{-3}$ ($1.0\text{x}10^{-4}$).

257 SPAR-H in this circumstance allows for expansive time, although stress and complexity can be argued to stay the same. The overall error probability will then be $4.0\text{x}10^{-4}$. Again, ASEP used as intended and SPAR-H are within a factor of 2.5 of each other.

Comparative Scenario 5: Complex Diagnosis Moderate Timescales

258 This scenario assumes that the fault will have been the subject of initial training (by definition this must be so if it is claimed within the safety case) but, being an infrequent fault, it will not be rigorously retrained. The timescales are one hour for diagnosis as in the previous example.

259 ASEP would suggest a nominal diagnostic error probability of $1.0\text{x}10^{-2}$ ($1.0\text{x}10^{-3}$) or $1.0\text{x}10^{-3}$ ($1.0\text{x}10^{-4}$) as previously. Whichever estimate is taken, it should be raised by a factor of 10, according to the method, because the event is not covered beyond initial training, i.e. to $1.0\text{x}10^{-1}$ or $1.0\text{x}10^{-2}$. In SPAR-H, the difference in training regime, which is reflected by ASEP, is not reflected in SPAR-H in a base case analysis. For a non-base case, low training provides a factor of 10 difference, exactly as for ASEP. Therefore, a base case ASEP provides a difference of $1.0\text{x}10^{-2}$ for ASEP versus $4.0\text{x}10^{-4}$ for SPAR-H: a difference of 25. However, if training is factored in to a full SPAR-H assessment then the difference reverts, once again to 2.5.

Overall Comparison of ASEP and SPAR-H for Diagnosis

260 It can be seen from the above examples that each method is sensitive to different qualitative factors and different results can be expected to arise in the assessment of diagnostic error. For short timescales, SPAR-H is always going to be optimistic relative to ASEP and may be up to an order of magnitude more optimistic. On intermediate timescales, the differences are sensitive to the qualitative factors that each of the methods invoke in their respective analyses. It can also be seen that SPAR-H base case assessment can lead to an optimistic assessment of reliability.

4.3.5.2 Comparison of ASEP with SPAR-H for Actions

261 Comparisons are made between ASEP and SPAR-H for action scenarios to illustrate and explore the differences between the two methods, in the same way as for the diagnostic scenarios above. All the following scenarios consider post-fault actions.

Comparative Scenario 1: Perform an Action under Moderate Stress

262 ASEP puts forward a screening probability of 5.0×10^{-2} (2.0×10^{-2}) for step by step task actions performed under moderately high stress. An error factor of five is applicable thereby suggesting an error probability range from 2.5×10^{-1} to 1.0×10^{-2}.

263 In comparison, SPAR-H for a base case provides a probability of 1.0×10^{-3}. Although it accounts for stress, it provides multipliers of two and five for high and extreme stress but no multiplier for moderate stress. It is interesting to note that these multipliers are identical to those given within THERP for which the corresponding qualitative descriptors are “moderately high” and “extremely high”. This appears to be something of a semantic confusion as it would be for the analyst to judge whether or not moderate stress should be rated as “high”. If one supposes that it is, then SPAR-H provides an estimated error probability of 2.0×10^{-3}. This is a factor of 25 more reliable than ASEP. However, unlike ASEP, SPAR-H allows the analyst to factor in available time and complexity as performance shaping factors, as with the diagnostic tasks. This is explored further in Scenario 2 below.

Comparative Scenario 2: Perform a Moderately Complex Action under Moderate Stress

264 In this scenario, the ASEP central estimate would be 5.0×10^{-2} (2.0×10^{-2}) as in scenario 1 above. However, the SPAR-H estimate would now be half as reliable giving an overall estimate of 4.0×10^{-3}. A difference of about one order of magnitude. However, if instead of being moderately complex, the tasks were considered highly complex, SPAR-H would still give a marginally more optimistic estimate than ASEP at 1.0×10^{-2}. The next scenario is engineered to show how SPAR-H will provide an estimate that is equivalent to ASEP.

Comparative Scenario 3: Perform a Highly Time Constrained Action under High Stress or High Complexity

265 In this scenario, the time available to perform the action is the same as the time required. This does not alter the ASEP estimate, which remains at 5.0×10^{-2} (2.0×10^{-2}). However, the SPAR-H estimate will now be 5.0×10^{-2} because a performance shaping factor of 10 is applied when the time available is the same as the time required to perform a task, bringing the estimate to 1.0×10^{-2}. A further factor of five is applied if high stress or high complexity is judged to apply. I conclude that SPAR-H only provides a calculated probability equivalent to the ASEP action probability when a combination of several negative PSFs applies.

266 The next scenario shows how SPAR-H can exceed ASEP in its estimate of error probability.

Comparative Scenario 4: Perform a Time Constrained Moderately Complex Action under an Extremely High Stress.

267 In this scenario, ASEP provides a central estimate of $2.5\text{x}10^{-1}$ ($5.0\text{x}10^{-2}$) as a function of stress, but is insensitive to complexity.

268 For the same scenario, SPAR-H postulates performance shaping factors of 10 for constrained time, five for stress and two for complexity thereby providing an overall estimate of $1.0\text{x}10^{-1}$. If complexity is rated as high, then SPAR-H and ASEP will provide identical estimates.

4.3.5.3 Overall Comparison of ASEP and SPAR-H for Post-fault Actions

269 The comparative scenarios illustrate that SPAR-H for a base case assessment will, in general, be up to an order of magnitude or more optimistic than an ASEP screening assessment for post-fault actions. The error estimates given by SPAR-H will equate with that given by ASEP only in instances where a time constraint, high stress and high complexity exist. Of course, if a SPAR-H assessment includes the other five PSFs then it becomes more likely that multipliers, particularly for poor ergonomics or procedures (which are 10 and 20 respectively) will increase error estimates.

270 These raise a fundamental issue about the application of SPAR-H, namely that the exclusion of factors in a base case assessment must mean that it has a tendency to be optimistic. However, the application of SPAR-H in the Level 2 PSA HRA includes the other factors. The logic behind this exclusion becomes debatable when it is common practice within the UK to predict the quality of ergonomics and procedures in advance of design completion. However, this exclusion has not been undertaken to the degree that would cause a SPAR-H assessment to equate to an equivalent ASEP screening assessment.

271 It should be noted that ASEP was always intended to be a more conservative method than THERP (Ref. 26). As SPAR-H has been benchmarked against THERP, this comparison suggests that SPAR-H is behaving in a manner intended by its developers: namely that is broadly consistent with THERP rather than ASEP.

272 I conclude that despite the inclusion of more qualitative factors for analyst consideration, SPAR-H will almost always provide a more optimistic assessment than an ASEP screening assessment for human reliability assessments of post-fault actions. The only exceptions to this will arise when several negative PSFs are identified by the analyst.

273 I therefore further conclude that the relative optimism offered by SPAR-H in comparison to the ASEP screening method, will proportionally tend to underestimate the human contribution to risk from the Level 2 PSA relative to the Level 1 PSA.

4.3.5.4 Overall View of the Level 2 PSA HRA Modelling

274 From the comparison of diagnostic and action tasks, along with issues relating to dependency, it becomes apparent that the relative contribution of the human to risk in the Level 2 PSA will be proportionally underestimated quite considerably relative to the Level 1 PSA. I use the phrase “proportionally underestimated” cautiously as it must be noted that the ASEP screening method has been used for the Level 1 PSA, which is intended to be conservative relative to the THERP benchmark method. In comparison, SPAR-H is

intended to perform in a closely similar way to THERP when estimating human error probabilities.

275 In practice, the higher levels of uncertainty associated with a Level 2 PSA make the application of screening methods more advisable than for a Level 1 PSA. I conclude that the same degree of conservatism has not been built into the Level 2 PSA as the Level 1. Accordingly, less attention may be paid to design interventions relevant to risk mitigation quantified in the Level 2 PSA than might be appropriate.

> ***AF-UKEPR-HF-13 –*** *The licensee shall ensure that identical actions are quantified by the same approach in both the Level 1 PSA and Level 2 PSA HRAs – or alternatively the licensee shall ensure that the HRA methods used for the Level 2 PSA HRA are not optimistic relative to the Level 1 PSA HRA assessments.*
>
> ***AF-UKEPR-HF-14 –*** *The HRA methods used for OSSA actions in the Level 2 PSA shall be fully justified and ensure qualitative insights are obtained for the development of OSSA guidance.*

4.3.6 Overall Treatment of Diagnosis in the PSA

276 The previous sections have shown the individual quantification methods used in the Level 1 and 2 PSA. Here I focus solely on the inclusion of diagnosis within the Level 1 PSA model. The PSA model and subsequent HRA assumes that the PICS system is always available, along with the AD feature. No consideration has been made of degradation or failure of the PICS system or AD feature.

277 The HRA has not undertaken any detailed consideration of the nature of diagnosis required, with and without AD support. It has now been recognised that a major failure of the PICS is a credible event that is likely to occur within the operational life of a UK EPR. This means that consideration of PICS degradation and failure needs to be undertaken, requiring consideration of diagnosis from alternative non-AD means of transfer to the SICS panel and diagnosis and action execution from it.

278 This lack of detailed consideration of diagnosis within the UK EPR is significant, as it is an essential part of the required substantiation of claimed post-fault safety actions. This deficiency is included within the GDA Issue that I have raised.

4.3.7 Assessment of Dependence within Human Failure Events

4.3.7.1 Assessment of Dependence within the HRA Supporting the Level 1 PSA

279 The methodology for the treatment of dependency used in the UK EPR HRA is outlined in NEPS-F DC-191 Human Reliability Analysis Notebook (Ref. 29). The methodology adopted for Level 1 PSA is that provided by ASEP. The UK EPR HRA Notebook describes the approach taken for the assessment of HEPs within the Level 1 PSA for three types of human errors:

- *HFE*s causing an initiating event.
- Pre-initiating fault *HFE*s.
- Post- initiating fault *HFE*s.

280 Treatment of each of these groups of human errors is assessed separately.

Initiating Human Failure Events

281 Five *HFE*s causing an initiating event are described in the Notebook (Ref. 29). Two of these are quantified on the basis of operational experience, whilst the remaining three are assigned HEPs of 1.0x10^{-2} and 1.0x10^{-1}, without any explanation of the derivation. A statement is made with respect to the assessment of dependency that *"No dependencies with subsequent post-accident actions are taken into account in the UK EPR PSA model."*

282 This statement, however, fails to address the issue of dependencies for the tasks within which the quantified *HFE*s occur. Indeed, the approach to HRA adopted for the *HFE*s is not based on any task analysis process and therefore the conditions that may affect human error likelihood, including dependency, are not explicitly assessed.

283 I judge that the assignment of HEPs for Initiating Human Errors is not based on an analytical process, and as a result the vulnerability to HED within and between initiating *HFEs* is unknown, and therefore the adequacy of the values derived cannot be properly assessed. This should be addressed in a revision of the HRA in the future.

> ***AF-UKEPR-HF-15 –*** *The licensee shall calculate the HEPs for initiating human errors based on an analytical process that includes consideration of dependency within the initiator and with other initiating HFEs.*

Pre-initiating Fault Human Failure Events

284 Pre-initiating fault *HFE*s are assessed using ASEP however, no assessment of dependence within the tasks is undertaken. Two claims are put forward in relation to this: that common cause failure assessment of the components which might be affected by human error accounts for human error dependence; and that maintenance and test procedures are performed according to procedures that aim to minimise the occurrence of dependent pre-accident errors. Neither of these claims is considered sufficient to justify the lack of a dependency assessment. Even if common cause failure data address quantitatively the effects of HED, a qualitative assessment of dependence is required in order to demonstrate that risk contribution of HED is managed consistent with the ALARP principle. With regard to the claim related to maintenance procedures, no evidence is provided to support the claim that the organisation of maintenance and maintenance instructions will minimise dependency between maintenance tasks. The ASEP pre-accident screening and nominal HRA methods both stress the importance of dependency assessment and provide simplified (in relation to THERP) dependency models for this.

285 I judge that further evidence is required to support the assertion that HED between pre-initiator *HFE* is minimised by maintenance and test procedures. This should be addressed as part of the HRA revision.

> ***AF-UKEPR-HF-16*** – *The licensee shall provide evidence to support the claims that maintenance and test procedures will minimise the potential for human error dependence.*

Post-initiating Fault Human Failure Events

286 Post-initiating event *HFE*s are assessed using ASEP (Ref. 26). No assessment of dependency effects is undertaken within the assessment of individual post-initiating *HFE*; each individual task is quantified by a single HEP, rather than breaking the task down into its individual sub-tasks and applying quantification at the sub-task level as would occur in a THERP analysis.

287 Although no explicit modelling of operator tasks and dependency between sub task steps is contained within the UK EPR HRA, assessment of dependence between individual

*HFE*s contained within a fault sequence is undertaken. For each individual *HFE*, the *HFE*s which share a dependency with it are identified. No explanation is given for the process by which these dependencies are identified, therefore it is not possible to assess the whether all dependencies are correctly identified.

288 I consider that further argument and evidence is required within the HEP derivation for individual post-initiator *HFE* in order to support the claims made with regard to the absence of dependency between individual *HFE*. This should be addressed as part of the HRA revision.

> ***AF-UKEPR-HF-17*** *– The licensee shall justify the assertion of zero dependency within sequences.*

289 Where dependence is identified to exist between *HFE*s, the level of dependence allocated between the *HFE*s is assigned on the basis of the THERP model. Five factors appear to be taken into account when allocating the degree of dependence between two tasks, these are:

- Location – whether the two tasks are performed from the same location (MCR or external).
- Time interval between the two tasks.
- Cues – whether both tasks depend on the same or different cues.
- System – whether both task involve the same or different system.
- Training – its frequency.

290 Whilst the coupling mechanisms used to allocate dependency levels are appropriate, there is a lack of systematic approach in how some of these variables are used to determine the correct level of dependence. This is most notable in relation to the variable of ‘time’. Here I would expect the analysis to identify specific time intervals between tasks related to each level of dependence, i.e. if the time interval between tasks is <5 minutes then high dependence is assigned, such as used in DEPEND HRA (Ref. 32). Similarly, I would expect to see a consistent consideration of the training variable such that clear criteria were established in relation to the different dependency levels.

291 Overall, I consider that appropriate coupling mechanisms have been used to allocate dependency levels, but that a more systematic application of the variables would improve the transparency of the dependency level allocations. This should be addressed as part of the HRA revision.

> ***AF-UKEPR-HF-18*** *– The licensee shall provide evidence of the application of a systematic consideration of coupling mechanisms relating to dependency level allocations within the HRA.*

4.3.7.2 Assessment of Individual Dependent Post Initiator Human Failure Events

OP_Bleed_30MIN

292 Failure to initiate feed and bleed within 30 minutes of an initiating event is identified as having a dependence on a previous *HFE* - failure to manually perform the partial cooldown. A medium dependency is claimed to exist between the two events. The claim for medium dependence, as opposed to high dependence, is based on the fact that requirement for the actions are signalled by different cues, that they involve different systems and that feed and bleed is a highly trained activity. However the two actions

occur at the same location (MCR), within a similar timeframe, and are likely to be required when the operators are in a state of high stress. This is used to argue that medium rather than low dependence be assigned to the dependent event. While the argument made is plausible, little evidence in the form of task analysis is provided to support it. Overall however, I consider that the allocation of medium dependence is appropriate given the information presented. The calculation procedures used to derive the conditional HEP are consistent with those prescribed in the THERP methodology (Ref. 20).

OP_FB_CA_120MIN

293 Failure to initiate feed and bleed within 120 minutes of an initiating event when in a shut down plant state, is identified to be dependent on a previous *HFE* - failure to start-up the standby Low Head Safety Injection/Residual Heat Removal (LHSI/RHR) train. Low dependency is claimed to exist between these two events. The rationale for the use of low dependence is based on the fact that, whilst both tasks are performed as part of the same sequence from the MCR, there is a time separation of up to 75 minutes between the two events, the requirement for the actions are signalled by different cues and that the actions are performed on different systems. On this basis the allocation of low dependence appears reasonable.

OP_FB_120MIN

294 Failure to initiate feed and bleed within 120 minutes of an initiating event, when in an at power plant state, is identified to be dependent on two previous events - failure to start manually or control the EFWS and failure to cross connect or re-feed the MFWS/EFWS tank. In this assessment it appears as though a sequence of three events is being considered: start of the EFWS, re-fill or cross connect the EFWS tank and feed and bleed. Thus it would appear that re-fill or cross connect the EFWS tank is dependent on its start-up and control, and that feed and bleed is dependent on re-fill of the tank. Thus two separate dependency assessments should be undertaken. Here, however, the dependency of feed and bleed on each of the EFWS tasks is assessed. This may result in an overly optimistic HEP for the sequence, as two independent and one dependent HEP are included, rather than a single independent HEP and two conditional HEPs.

OP_LHSI/COOL_2H

295 Failure to start-up the LHSI in injection mode at shutdown is identified as having a dependence on start-up of the standby LHSI/RHR train. Low dependency is claimed to exist between the two events principally due to the long time interval (up to 105 minutes) between the two events, and the availability of different cues to signal the need for the actions. On this basis the allocation of low dependence appears reasonable. OP_LHSI/COOL_2H_MDEP and OPE_52_LDEP provide similar examples of dependent *HFEs* for loss of cooling events in shutdown states.

296 From the above examples and other *HFE*s examined, I judge that the dependency levels that EDF and AREVA have applied in the HRA are generally reasonable based on the assumptions provided in their analysis. However the HRA needs to undertake appropriate qualitative assessment of the tasks in order to determine and justify the dependency levels. This should be addressed as part of the HRA revision.

> ***AF-UKEPR-HF-19 –*** *The licensee shall qualitatively substantiate the dependency levels applied within the HRA.*

Cutset Analysis

297 An analysis of the top 67,195 cutsets is reported in NEPS-F DC 191 (Ref. 29) which indicates that 88% of the cutsets contain none or only a single human error. 10.5% of the

cutsets contain two human errors and the remaining 1.5% of cutsets contain three human errors. No cutset contains more than three human errors. The cutset analysis identifies six cutsets containing two human errors with total HEPs in excess of 1.0x10^{-4}; HEP values ranging between 4.3x10^{-6} and 2.4x10^{-5}. In each of these cases a justification for the low HEP value is provided, based on either the long time scale between the human actions, or the fact that the human actions form part of a different operation. A sensitivity analysis demonstrates that manipulation of the level of dependence for all cutsets has only a small effect on the Core Damage Frequency (CDF), which suggests that the use of such low HEPs in the PSA has a very limited impact on CDF.

298 Furthermore, five of the cutsets have an overall HEP lower than 1.0x10^{-5}. The TAG on HRA (Ref. 7) recognises the internationally accepted 'limit' for HEPs in any accident sequence/cutest of 1.0x10^{-5}, and states that *"Where a value approaching 1E-05 is offered, the dutyholder should provide a robust, modern standards qualitative substantiation to support such a value, and there should be a clear and rigorous demonstration of task feasibility and optimised conditions for human performance. ONR would not ordinarily expect to see reliance on human reliability claims of this order being made, as this would suggest inadequacy in the dutyholder's defence in depth strategy and that the balance of protection is potentially inappropriate."* This should be recognised and addressed as part of the HRA update.

299 For cutsets containing three human errors, the majority have a total HEP contribution higher than 1.0x10^{-3}. Three cutsets however have total HEPs lower than this. Where total HEP values for a cutset are lower than 1.0x10^{-3}, two of the total HEP values are greater than 1.0x10^{-5}. A single cutset has a total HEP value of 9.1x10^{-7} which is well below the range internationally accepted within the HRA community. This will require revision in the update to the HRA. In addition, whilst justification is provided that no direct dependency exists between the three human error events contained within the cutset, the issue of indirect dependency is not considered and this should be addressed as part of the HRA revision.

300 Overall, I judge that the consideration of *HFE*s within cutsets is broadly acceptable and has not led to excessive claims for multiple operation actions. However, I consider it appropriate that total cutset values lower than 1.0x10^{-5} be reconsidered and revised as part of the HRA update.

> ***AF-UKEPR-HF-20*** *– The licensee shall identify multiple operator actions within cutsets and reconsider and justify those where the combined HEPs are lower than 1.0x10^{-5}.*

4.3.7.3 Assessment of Dependency within the HRA Supporting the Level 2 PSA

301 Within the Level 2 PSA, the primary technique used for the HRA is the SPAR-H method. This also forms the basis for the treatment of dependency in the majority of situations. *HFEs* in the Level 2 PSA are modelled using OSSA which is a less prescriptive strategy based on operator support involving a number of disparate groups of operators and supervisors who work together to deal with a severe accident condition. Within the HRA supporting the Level 2 PSA, three potential sources of dependency are considered. These dependencies are:

- Within individual steps making up an OSSA action.
- Between Pre-OSSA and OSSA actions.
- Between OSSA actions.

302 Document NEPS-F DC-527 UK EPR Level 2 Supporting Human Reliability Analysis (Ref. 30) describes the approach taken for the assessment of dependency in each of these situations.

Treatment of Dependency within an OSSA Action

303 Each of the individual tasks making up a single OSSA action is separated into eight separate steps. These are:

- Identification of concern.
- Hardware evaluation.
- Impact evaluation.
- Strategy recommendation.
- Strategy authorisation process.
- Strategy implementation.
- Strategy verification/evaluation.
- Strategy long term maintenance.

304 These individual task steps typically involve communication between two groups of the different OSSA response groups dealing with the severe accident condition modelled in the PSA. The eight steps outlined above are considered to be sequential and dependencies between successive task steps are modelled in two event trees which include the level of dependence at each step in the sequence. Levels of dependence used in the event trees are those provided by the THERP dependence model, with the THERP equations being used to derive conditional HEPs once a level of dependence has been assessed. Two separate event trees and associated equations for deriving final HEPs are provided; one for severe accident scenarios that do not involve voluntary release, the second for those requiring voluntary releases. Although the general approach to modelling dependence between the individual task steps in an action appears to be consistent with good practice, there is little explanation or justification provided for the level of dependence at each branch of the event tree, other than a statement that the dependence level is a function of the nature of the relationship and the communication between the individuals who interact at each decision step. Further justification is required for each level of dependence used within the event trees and the equations used to derive the total HEP for each individual OSSA action.

> ***AF-UKEPR-HF-21 –*** *The licensee shall provide a comprehensive justification for the allocation of levels of dependence for OSSA actions modelled in the Level 2 PSA.*

Treatment of Dependency between Pre-OSSA and OSSA Actions

305 Treatment of dependencies between Pre-OSSA and OSSA actions is undertaken using the decision trees contained within SPAR-H for allocating levels of dependence. Dependencies between the following Level 1 PSA *HFE* and OSSA *HFE* are evaluated by application of the decision SPAR-H decision tree:

306 Level 1 *HFE* – failure to -

- Start feed and bleed.
- Initiate fast cooldown.
- Initiate RHR.

- Start EBS.
- Connect and load SBO Diesel Generators.

307 Level 2 *HFE* – failure to -

- Manually initiate containment isolation.
- Transition from EOP to OSSA.
- Depressurise the primary system before the Reactor Pressure Vessel (RPV) fails (25min / 65min).

308 Dependencies are also evaluated between two Level 2 Pre-OSSA actions and some of the early Level 2 OSSA actions listed above. The two level 2 Pre-OSSA actions are:

309 Level 2 Pre OSSA *HFE* – failure to -

- Manually initiate containment isolation.
- Depressurise the primary system before the RPV fails.

310 Results of the dependency evaluation are reported in Table 11 of NEPS-F DC-527 with conditional HEPs for the OSSA actions reported in Table 13. The allocation of dependency levels are discussed in relation to each of the four dependency coupling mechanisms used in the SPAR-H dependency decision tree. The assignment of dependency levels is transparent and is consistent with good practice and the conditional HEPs are calculated correctly.

<u>Treatment of Dependency between OSSA Actions</u>

311 Treatment of dependencies between OSSA actions is also undertaken using the decision trees contained within SPAR-H for allocating levels of dependence. Dependencies between ten OSSA actions are evaluated using the SPAR-H decision tree. These are:

- Operators fail to depressurise the primary system before the RPV fails.
- Operators fail to start safety injection for in-vessel recovery following depressurisation by the operator.
- Operators fail to start safety injection for in-vessel recovery following hot leg rupture.
- Operators fail to start the Containment Heat Removal System (CHRS) spray to depressurise the containment.
- Operators fail to switch to active cooling of the corium in the pit after successful spray actuation.
- Operators fail to use safety injection as a back-up for the CHRS for active cooling of corium in the pit.
- Operators fail to switch CHRS to active cooling of the corium in the pit after hardware failure of the sprays.
- Operators fail to restart CHRS spray after hardware failure of active cooling.
- Operators fail to actuate CHRS sprays to mitigate early releases for cases where containment isolation failed.
- Operators fail to actuate CHRS sprays to quench the source term and mitigate releases.

312 Results of the dependency evaluation are reported in Table 12 of NEPS-F DC-527 with conditional HEPs for the OSSA actions reported in Table 13. The allocation of dependency levels are discussed in relation to each of the four dependency coupling mechanisms used in the SPAR-H dependency decision tree. Again, the assignment of dependency levels is transparent and is consistent with good practice and the conditional HEPs are calculated correctly.

4.3.7.4 Dependency Conclusions

313 In general I am content that the treatment of dependence uses appropriate methods that are consistent with good practice and regulatory expectations. However, for the Level 1 PSA, particularly with respect to pre-initiator and initiating *HFEs*, I would characterise the HRA as an assumptions based screening analysis rather than a best estimate HRA based on task analysis. The lack of qualitative analysis to substantiate HRA claims is addressed in GDA Issue **GI-UKEPR-HF-01**. As discussed earlier I expect the HRA revision for the Level 1 PSA to be much more detailed and be based on task analysis, including the consideration of dependencies.

314 For the HRA supporting the Level 2 PSA, I am broadly satisfied with the treatment of dependence, although a clearer justification of the levels of dependence applied in the equations used for the derivation of total HEPs for each *HFE* is required to support the analysis of within *HFE* dependence. This should be addressed as part of the HRA revision.

> ***AF-UKEPR-HF-21 –*** *The licensee shall provide a comprehensive justification for the allocation of levels of dependence for OSSA actions modelled in the Level 2 PSA (repeat)*

4.3.8 Spend Fuel Pool HRA – HCR Application

315 EDF and AREVA have included claims for repair within the spent fuel pool accident scenario assessments (Ref. 34) for the PSA using the Human Cognitive Reliability (HCR) method (Ref. 35). I have considered the suitability and application of this method for this PSA.

316 The spent fuel pool accident scenarios are analysed using the event tree approach described in the PSA documented in NEPS-F DC 355 B FIN (Ref. 34). The event trees for the accident scenarios that are not rapid drain-down scenarios, include branch points for *HFE*s that represent the success or failure of the operators to initiate mitigation strategies for the loss of spent fuel pool cooling. The probabilities for these *HFE*s are estimated using the same approach as for the internal events PSA. In addition, as stated on page 1129 of Reference 34: *"… in case of failure of I&C indications and failure of activation of the makeup countermeasures by the operator, the possibility to repair failed components are taken into account for non-refuelling states (the time window is about 107 hours). For the refuelling states, as the time window is about 30 hours, it is conservatively assumed that the failure of I&C followed by the failure of makeup actuation by the operator would directly lead to core damage."* I note that the event trees include recovery events for accident sequences during refuelling states also, albeit with less credit (~0.1 vs. 1.0x10^{-3}). (Refer for example to Appendix DR1.4, page 1452 of Ref. 34.)

317 The HCR method is only applied to failure to repair as the final event on the event trees for the non-refuelling and refuelling states. They are applied to all potential core damage states, whether the previous events are operator failures or not. The actual equipment to

be repaired is not specified, and the same recovery factor is used for all sequences, regardless of the initiating event. Furthermore, it is assumed that the equipment to be repaired is accessible, even in the case of steaming from the fuel pool into the fuel building (page 1131 of Ref. 17).

4.3.8.1 The Human Cognitive Reliability Method

318 The HCR correlation was proposed in 1984 (Ref. 35) as a method to estimate the probability that a control room crew would respond to a plant event within a specified amount of time. Specifically, the correlation describes the time taken to initiate an activity. It was not intended to include the execution phase of the response and therefore provides an incomplete assessment of the HEP associated with a *HFE*. The correlation was structured to take into account a) the types of human behaviour that can result in significantly different response times; and b) situational factors and crew characteristics that can influence the response time.

319 In 1990, the Electric Power Research Institute (EPRI) published a report (Ref. 36) describing the results of an examination of the validity of the Human Cognitive Reliability (HCR) correlation using data from full-scale nuclear power plant simulators. The research program was called the Operator Reliability Experiments (ORE). The conclusions of the study resulted in the reformulation of the HCR correlation into the HCR/ORE correlation

4.3.8.2 Significance of the Repair Claim

320 The repair term is applied only to the loss of fuel pool cooling scenarios, which accounts for 3% of the total frequency of fuel damage in the spent fuel pool cooling system, which is $2.4\text{x}10^{-9}$/reactor year. Therefore, the contribution to CDF from loss of fuel pool cooling scenarios, taking credit for repair, is $7.2\text{x}10^{-11}$/ reactor year. While I was not able to find an importance analysis for the overall impact of the events, since the maximum credit taken for repair is in the order of $2.0\text{x}10^{-3}$, the maximum impact of not taking credit for repair is to increase the total fuel damage frequency for spent fuel pool accidents to about $3.8\text{x}10^{-8}$/reactor year, which is of the order of 5% of the total CDF from all accidents.

4.3.8.3 General Conclusion of Spent Fuel Pool HRA

321 I consider that the use of the HCR correlation to estimate the probability of repair is inappropriate for two reasons. There is neither a theoretical or empirical basis for the correlation used in HCR. It was intended to represent the variability of crew responses in initiating a response to a plant event and does not include execution of the selected action. I judge that detailed consideration of the repair actions is necessary to determine their likely reliability. Additionally, there has been no consideration of the potential for dependency between the failure to repair and prior *HFE*s in the same accident sequence.

322 The same probability of failure to repair is used for all initiating events and for all functional failures. I do not consider this to be realistic. Repairs of failures, for example complex components, are certain to be more difficult and time-consuming than more simple ones.

323 I judge that some credit for repair actions in the long term is credible, but that the assessment of such actions for the HRA revision,should be based on more detailed consideration of the actual repair claims, and include consideration of dependency.

4.3.9 Conclusions

324 From my assessment it is evident that the current UK EPR HRA is essentially an 'assumptions based' HRA that lacks adequate substantiation from appropriate task analysis of pre- and post-fault operator actions. However, I judge that an acceptable quantitative consideration of the contribution of operator error to overall plant risk has been made at this point. This is based on several factors namely:

- Type A and B error contributions are adequately included in the numerical estimates for both systems reliability and fault frequencies for overall risk estimation at the PCSR stage.
- The post-fault demands for operator actions are broadly similar to previous PWR plants.
- Discussions with my PSA colleagues on the adequacy of the HRA modelling and results of sensitivity studies on the human based safety claims.

325 The HRA is generally conservative and the claims appear reasonable and capable of being substantiated, or amended acceptably, without requiring significant design changes to major structures and systems.

326 I consider that the HRA methods used for the Level 1 PSA have generally been satisfactory, although there needs to be greater consideration and inclusion of pre-fault actions (both Type A and B), and an approved consideration of dependency when the HRA is revised, based on detailed qualitative analyses.

327 The consideration of human failure initiating events, particularly for low power and shutdown states, appears to be incomplete. Based on past PSA experience, this could be significant; it is an important area to ensure that the design is ALARP.

328 I judge that the detailed application of SPAR-H for the Level 2 PSA HRA has not been adequately justified and this should be addressed in the future HRA revision. The particularly areas for attention are the:

- Modelling of the OSSA roles;
- Potential optimism relative to the Level 1 PSA HRA for the same/similar actions.
- Event tree logic underpinning the SPAR-H assessments.
- Detailed consideration of dependency within an individual *HFE*s.

329 Annex 4 provides additional details of my Work Stream 2 assessment.

4.4 Work Stream 3: Engineering Systems - Assessment

330 In Section 18.1.3 of the November 2009 PCSR (Ref. 17) EDF and AREVA claim that the HFE programme considers HF within the design of the EPR and that HFE programme covers maintenance activities. This includes the following key statements:

"Human Factors is taken into account in the EPR design, especially when the tasks to be performed are associated with nuclear safety, and when the working environment may be dangerous for personnel. The HFE programme therefore applies mainly to operational activities (including equipment isolations and testing), technical logistics (scaffolding ..) and maintenance. Testing is covered both by operational and maintenance activities."

Maintenance activities

With regard to future maintenance work, and given the number of possible situations, the HFE programme is applied to a selected number of situations and activities. For these activities, the HFE programme covers:

- *The layout of the plant buildings and of the facilities installed in them. This includes issues such as equipment access, personnel access routes, and handling devices required for maintenance activities.*
- *Working environment conditions: acoustic, lighting, temperature, and humidity.*

In broad terms, the HFE programme is based on:

- *A fundamental methodology, described in Section 2.1 of this sub-chapter, which is applied to the principal working situations, each with its own imperatives (safety, security, radiological protection and availability).*
- *Investigations of specific areas (e.g. radiological protection), supplemented by the programme.*
- *A set of rules to be applied during design."*

331 This section explores the robustness of these claims and arguments against the evidence presented. The majority of this work stream is focused on maintenance and maintainability. However, I have also considered human reliability issues associated with software maintenance.

4.4.1 Maintenance / Maintainability

332 These findings relate to item (1) from the methodology and scope presented in Section 3.2.7. EDF and AREVA state in Section 18.2.1 of the November 2009 PCSR that they use a four stage process for the HF contribution to maintenance/maintainability:

- Analysis of existing situations.
- Contribution to specifications.
- Specification of plant designs.
- Adjustment of design specifications.

333 I have considered the key elements of these four stages and a summary of my key findings is presented below.

4.4.1.1 Operational experience

334 EDF and AREVA make a number of claims regarding their use of operational experience relating to the HF aspects of maintenance. The following statements are made in the November 2009 PCSR sub-chapter 18.1 (Ref. 17).

"Human Factors (HF) have been given due consideration throughout the design stage, taking into account aspects of operation, testing and maintenance, with particular emphasis on operating experience."

> "*The first stage in incorporating HF in the design is to identify and analyse feedback from situations at existing plants. The purpose of this review is to identify and analyse HFE-related problems and issues in previous similar designs so that problem areas can be identified and previously successful design features can be retained.*"

335 In terms of maintenance EDF and AREVA state in the PSCR sub-chapter 18.1 (Ref. 17). that, *"…operating feedback experience from existing plants is the first step in the taking Human Factors into account in the design of maintenance areas*" Additionally, they claim that the following areas will be considered: equipment access, personnel access routes, handling methods, storage, tools, identification, working environment (e.g. noise, temperature, lighting) and communications.

336 Specifically, in terms of maintenance and location, EDF and AREVA have provided a limited number of examples to highlight how they have applied OEF to the design of local maintenance operations. In particular:

- An EDF study focusing on the N4 plant series in 2002 (Operating Feedback Study on the N4 plant series for EPR – Local activity at Chooz NPP (Ref. 49)).
- Operating feedback from specialists in the Nuclear Power Generation Division seconded to Centre National d'Etudes Nucléaire (CNEN) for the project, with knowledge of significant events and their own personal experience.
- 'Ergonomic' studies into the actual work performed for activities identified on an issue-by-issue basis, e.g. on Fuel Handling (Ref. 50) and radiation protection (see below).

337 For example the Chooz Operating Feedback Study states that its main purpose was to *"…identify operating feedback relating to maintenance and operating activities in N4 series facilities (excluding the control room)"*. The aim of the study was, therefore, to identify difficulties encountered by workers and determine the design choices that resulted in these difficulties and to indentify positive aspects of design that led to advantageous working conditions. EDF and AREVA state that around forty people were interviewed including field workers, tagging supervisors, operating technicians, preparation assistants and external service providers to explore the following topics:

- Space (cramped conditions, under-sizing etc).
- Location of rooms (distance, spread etc).
- Accessibility (rooms, equipment).
- Handling and lifting operations (anchor points, lifting equipment and bridge cranes, elevators, hatches etc).
- Storage (areas provided for storage).
- Signposting (rooms, equipment, maintenance of labels etc).
- Working environment (heat, noise etc).
- Communications (systems available, reliability etc).

338 There is a lack of evidence that describes the detailed design outcomes and design choices or requirements that resulted from this study. However, from my consideration of the design, it does appear that the OEF has been taken into account even though the process appears *ad hoc.* For example the adoption of fast assembly-disassembly thermal insulation and the adoption of modular-maintenance globe valves in radioactive systems (Ref. 51).

339 Overall, I judge that EDF and AREVA have used operational experience and analysis of previous plants as a useful design input for the UK EPR. However, there is a lack of evidence relating to the overall selection process for areas to assess in detail and how the studies have explicitly addressed equipment ergonomics relevant to maintenance/maintainability (rather than basic layout, space, access, provision of lifting/movement facilities). I recognise that EDF and AREVA have provided a substantial volume of additional documentation very late in Step 4, including additional examples in this area. Unfortunately, I have not been able to consider much of this late material in my Step 4 assessment.

4.4.1.2 Design for Maintenance/Maintainability

340 EDF and AREVA state in Section 18.2.2 of the November 2009 PCSR (Ref. 17) that maintenance is considered at two different stages of specification.

- Functional specification - for all buildings; these include consideration of plant layout and definition of requirements including equipment layout. Requirements are claimed to incorporate previous experience.
- Detailed specification – where detailed HF contributions are included.

341 EDF and AREVA have not produced detailed HF requirements documents for each system and equipment specification; HF requirements have been integrated into other technical requirements documents. This is potentially an acceptable approach subject to the adequacy of the HF scope.

342 I note that many HF requirements are included in buildings requirements documents. However, based on my review of a selection of EDF and AREVA's documentation, the quality of the integrated guidance is variable and often at a level that, whilst sensible, is insufficiently prescriptive to adequately and practically aid a designer. For example [taken from Meziere, A. and Bily, P. (2009) Reactor Building Specifications - ECIG0001089 (Ref. 52)]:

"Access to all components that require handling or monitoring by an operator must be facilitated, taking into account the most up-to-date knowledge in ergonomics."

"Lighting design and the light-coloured paints chosen for the walls shall be such as to ensure a good level of light intensity."

"The noise level must be compatible with the quality and complexity of the operating tasks performed in the rooms."

"Temperature - The rooms must be kept at a suitable temperature.

The equipment and characteristics of work areas must be suitable to the temperature of the human body during working hours, taking into account the working methods and physical stress undergone by the workers."

"With maintenance in mind, operation must incorporate some specific rules, as follows:

- *equipment should be accessible on a single level, both handling components and monitoring components,*
- *signposting should be implement to facilitate personnel access to maintenance sites"*

“Designers shall likewise draw on international experience, on research into previous decommissioning operations and on current research and feedback from major dismantling operations in France in the designs for cleaning protective equipment.”

“Special attention shall be paid to the comprehensibility of messages broadcast, in particular alarms.”

“In the event that insulation lagging has to be removed, double-labelling should be used as a marking system to avoid any errors during reassembly. Insulation storage areas shall be provided and marked out.”

343 There are further examples of vague guidance in other documents reviewed, for example ‘EPR – Technical Specifications for the Diesel Buildings’ (Ref. 53).

344 There is however, more useful guidance relating to the overall workplace design, including accessibility and provision of equipment. For example, the “Reactor Building Specifications” (Ref. 52) specifies that:

“At least 600mm clearance must be allowed all around components that will require in-service inspection or maintenance (around 3 sides at least for small components).”

“It must be possible to handle equipment items without having to disassemble other equipment.”

“The various communication networks used by the operator must cover all the rooms with the systems used, ensuring the public address system is audible and that sockets at every level provide access to the IT network.”

345 This more prescriptive guidance minimises the likelihood of future issues arising when the detailed equipment is designed and provided, which cannot readily be accommodated within the basic building design.

346 EDF and AREVA also state that, in addition to these building guides (which communicate a wide spectrum of requirements) further support is provided by specific equipment documents. For example: ‘Book of Technical Specifications for NPP Valves’ (Ref. 54). This document makes recommendations on how to optimise maintenance. For example: *“Modular” Maintenance: Adoption of interchangeable sub-assemblies (pre-adjusted, tested and pre-calibrated in the workshop before the work) and for which installation on the equipment consists solely of a simple operation (assembly between flanges, removable seat such that the body can be left in place, etc.).”*

347 I have only been able to assess a very limited number of these equipment level guidance documents as they were submitted late in GDA Step 4. My initial judgement is that they are similar to the buildings specification documents in that they contain some useful information but appear to lack precision on relevant HF aspects. For example, the NPP valves specification (Ref. 54) omits issues such as access envelopes, torque limits for manual operation and the use of keyed valve handles to ensure the handle can only be replaced in the correct orientation.

348 In addition, further sources of requirements for the design process are the Installation Rules Datasheets (DRI). According to EDF and AREVA, these provide guidance to the designer on a range of subjects. They were developed by working groups, following a specified format to review the rules and align them with current practice. They also take into account operational experience. EDF and AREVA claim that these datasheets will help to facilitate maintenance, operational and accessibility considerations to be incorporated into the EPR installation design.

349 I was able to observe a number of DRI documents during an inspection and my initial judgement, based on a very brief review, is that they do provide design rules applicable to HF engineering and maintenance issues, such as equipment design and space requirements.

350 Two key claimed elements of verifying the requirements and their implementation are the design review meetings and installation checks using the 3D Computer Aided Design (CAD) model.

351 EDF and AREVA state that during the design phases, installation review studies are carried out, which are led by EDF building specialists. The aim of these studies is to monitor the contractors carrying out installation studies and design work. EDF and AREVA state that HF specialists are involved in establishing the requirements of this installation review process, to ensure that HF considerations are taken into account.

352 EDF and AREVA cite a number of documents (Refs 55, 56, 57 and 58) as evidence of this review process and to demonstrate that HF is integrated into the design phase. At the time of writing however, these documents were only provided in French and hence I have not assessed them.

353 During my inspection, EDF and AREVA described how they use the 3D CAD models to review space requirements for planned maintenance activities and to support a series of ‘layout studies’. These are scheduled review meetings undertaken for facility areas and attended by HF. They aim to ensure that design rules are being applied, discuss any emerging issues and resolve any potential conflict. However, I have not seen evidence to demonstrate the actual extent of use of the 3D CAD model, or how well HF aspects have been considered. EDF and AREVA advise that evidence is included in submissions received too late to include in my assessment.

354 In addition, work undertaken in the radiological protection area to reduce operator dose limits using OEF (Ref. 59), could potentially result in an overall reduction in the maintenance requirements and hence the maintenance error potential. There is evidence of a HF contribution to this work.

4.4.1.3 Software Maintenance

355 The UK EPR places a greater reliance on automated systems and Visual Display Unit (VDU) based soft controls, than earlier generation plants. This typically presents different (latent) human error modes for consideration and mitigation. My interest at this stage of the design (PCSR) is the human reliability issues associated with the first installed software relating to control and protection systems. My interest is purely from a process perspective during GDA; that EDF and AREVA are applying a recognised software development system that acknowledges the potential for human error and provides the necessary mitigation.

356 EDF and AREVA provided a document containing technical specifications and conditions (Ref. 60) for future Control and Instrumentation (C&I) systems, which includes requirements for operation and maintenance. For example there are requirements on suppliers of C&I equipment to specify:

- The schedule for regular preventative maintenance.
- Detection and annunciation (e.g. operators are alerted at the earliest to system failures or deviations, performance degradations).

- System monitoring (e.g. contractor must specify the monitoring which must be performed on the system to detect system failures and deviations).
- Diagnostic functions (e.g. system must have detailed diagnostic functions for the relevant service equipment for identifying the root cause of failures detected by the system).
- Locating components to be replaced (e.g. the system must be designed to facilitate identification of components which must be replaced. The contractor must specify the mechanisms implemented to achieve this).

357 In addition, the document details requirements for on-site maintenance; maintenance action procedures; system availability during maintenance; system behaviour during maintenance; error avoidance during maintenance activities; standard exchange of hardware components; reloading data; personal safety; and system configuration modification.

358 I have consulted with my C&I colleagues and their assessment has not identified any problems relating to software maintenance at this stage. I note that they are seeking additional work to provide confidence in aspects of the software safety case (**GI-UKEPR-CI-03**, see Ref. 156), including rigorous testing of the TXS software system for GDA.

359 I have worked with my C&I colleagues to understand the software development process and standards employed by EDF and AREVA. With their help I have gained a level of confidence that the standards adopted by EDF and AREVA typically provide opportunities for human errors to be identified and recovered. Therefore, at this stage of the risk assessment I do not consider that there are any HF issues associated with the EDF and AREVA approach to the development of the first installed software process. Post-GDA, my interest will relate more to the control of software upgrades and changes

4.4.2 Conclusions

360 I consider that EDF and AREVA have integrated relevant operational experience to maintenance/maintainability. However they have not demonstrated a coherent approach for the areas selected for detailed study, nor have they demonstrated that the operational experience consideration has systematically considered all relevant aspects of HF for maintenance.

361 I judge that HF has been embedded in design requirements and guidance. However, this appears to have been limited primarily to workplace layout, particularly workspace, access, provision of support facilities and personnel safety. There is little evidence of a systematic application of detailed HF guidance at system and equipment level, which places considerable reliance on later verification and validation studies to ensure that the designs are satisfactory.

362 Overall, I judge that EDF and AREVA's approach for maintenance/maintainability is likely to be adequate to ensure that the main building designs are acceptable in terms of the footprint, such that any equipment design changes are likely to be accommodated within the overall plant layout.

> ***AF-UKEPR-HF-22*** *– The licensee shall ensure that the adequacy of HF maintenance and maintainability requirements is explicitly addressed in their V&V programme.*

363 Additionally, for the UK EPR design, a future licensee should enhance the detailed systems and equipments specifications requirements to incorporate more precise HF requirements.

> ***AF-UKEPR-HF-23 –** The licensee shall ensure that the system and equipment design specifications contain a detailed set of HF requirements and are based on recognised standards where appropriate.*

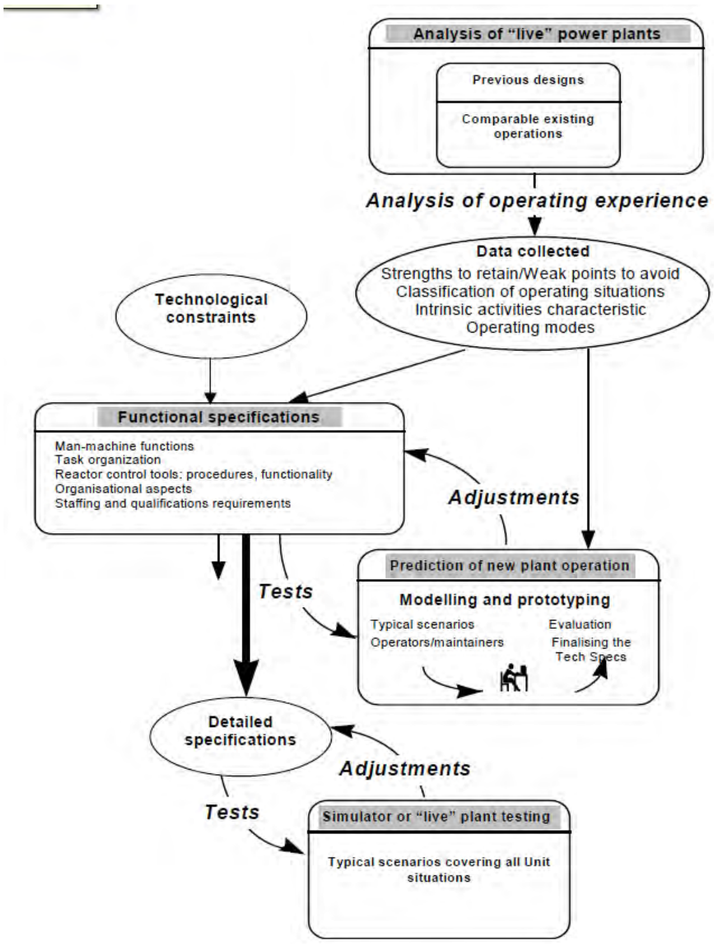
4.5 Work Stream 4: Human Factors Integration - Assessment

4.5.1 Overview

364 This aspect of my assessment has drawn upon over sixty reference documents. In addition, a substantial amount of documentation was submitted very late in Step 4 (with the response to TQ-UKEPR-1026); much of it in French, and I have only been able to sample a small part of the material submitted.

365 EDF and AREVA outline their approach to HFI in Section 18.1 of the November 2009 PCSR (Ref. 17) and in the '*Approach for Integration of Human Factors in EPR Design'* (Ref. 62). This claims that an iterative approach has been applied, based on analysis of the existing situation (on operating plants). Refer to Figure 3 below, taken from Ref. 62.

Figure 3: The EDF and AREVA "iterative" Approach in Principle


Analysis of "live" power plants
Previous designs
Comparable existing operations
Analysis of operating experience
Data collected
Strengths to retain/Weak points to avoid
Classification of operating situations
Intrinsic activities characteristic
Operating modes
Technological constraints
Functional specifications
Man-machine functions
Task organization
Reactor control tools: procedures, functionality
Organisational aspects
Staffing and qualifications requirements
Adjustments
Tests
Prediction of new plant operation
Modelling and prototyping
Typical scenarios
Operators/maintainers
Evaluation
Finalising the Tech Specs
Detailed specifications
Adjustments
Tests
Simulator or "live" plant testing
Typical scenarios covering all Unit situations

366 My initial examination of the evidence revealed that the documentation did not encompass the breadth of HFI expectations covered by the HFI TAG (Ref. 7). There is evidence of a HFE programme of work but it is largely focused on the MCR design. I have found little evidence of a fully integrated programme that actively works with other related technical disciplines in a cohesive manner to optimise the design, and from that optimisation develop and iterate the safety analysis. In addition, although the major components of a recognisable HFI programme are evidenced there are significant omissions. There has been a considerable reliance on the use of operational experience with little underpinning HF analysis. In my opinion, this does not necessarily result in an ALARP position and I have discussed this earlier in this report.

367 A recognisable HFI plan will be required for any UK EPR construction.

> ***AF-UKEPR-HF-24 –*** *The licensee shall develop and submit a HFIP for UK EPR construction.*

368 This section explores the claims, arguments and evidence of the key HFI TAG expectations.

4.5.2 Scope of Human Factors Integration

4.5.2.1 Breadth of Human Factors Integration Programme

Human Factors Integration Plan (HFIP)

369 TAG T/AST/058 (Ref. 7) offers specific guidance on the scope and content of a HFIP, which is the key management document that drives the HFI process. This defines how the project will be carried out, when, and by whom. The guidance states:

"The assessor should ensure that a project specific HFIP is developed during the initial phases of the project. This is the key document that describes in detail how human factors issues will be integrated and managed through the project. However the HFIP should be a living document that is able to evolve and reflect any changes over time relating to safety significant human actions."

370 It further states:

"Assessors should ensure that the following information is captured in the HFIP:

The strategy for integrating HF with other disciplines, including cross discipline working and communications within the project and with contractors;

- *A project organogram highlighting the position of the HF lead;*
- *The work breakdown structure of the HF analysis throughout the project (what HF analysis work is to done, at what level of detail, and when in the project);*
- *Integration of HF within the project plan. This should detail the key HF deliverables and show dependencies between discipline outputs;*
- *HF SQEP resource requirements and how that resource will be managed;*
- *The HF standards to be applied;*
- *How assumptions, uncertainties and project issues and risks will be managed and resolved;*
- *How trade-offs between different discipline requirements will be managed and resolved;*

- *Hold points and design reviews and the expected HF contribution;*
- *Who has ownership of particular aspects of the work;*
- *Progress monitoring arrangements; and Reporting methods"*

371 My assessment of Ref. 62 showed that it falls substantially short of the above requirements. However, EDF and AREVA claim an alternative approach to the HFIP where HF good practice is encapsulated within their various design specification documents, which mitigates the requirement for an integration management document such as an HFIP. These requirements are essentially embedded in the various design guidance and requirement documents applied at various points in the process shown in Figure 3.

372 I have not found any detailed documentation regarding the scope of both plant and HF aspects covered by the 'embedded' approach described by EDF and AREVA. Nor have I found any evidence of a systematic process for determining the level of HF attention provided to any part of the plant design. It is evident that detailed studies have been undertaken for some aspects of the plant (e.g. Fuel Handling (Ref. 50)), although the scope and selection criteria for those areas receiving greater attention are not clear.

373 Due to the late submission of the evidence for EDF and AREVA's HFI approach, I have found it difficult to verify the overall adequacy of their approach. Whilst many of the supplied references do contain some HF guidance, it is generally limited, often at the principle level, and relies on international standards to inform the design, rather than detailed prescriptive requirements that would be expected if following good practice. This should be addressed as part of the response to AF 24 cited earlier.

Organisation and Resource

374 TAG T/AST/058 (Ref. 7) requires that the HF team is embedded within the project team to ensure HF receives appropriate focus and influence on the project. It also indicates that HF analysis is undertaken by suitably qualified and experienced persons (SQEP).

375 EDF and AREVA have provided an organogram (Ref. 63) and information on the organisation and resourcing of HF work for the FA3 (reference) design. This indicates that there is a single HF coordinator and two additional full time HF engineers, along with one part time, all of whom work for EDF Research and Development. Additional sub-contract support is claimed to be available as needed. With respect to the organisational structure of the team, I note that the EDF Research and Development HF engineers are embedded within the CNEN design teams, which is in line with UK good practice. These engineers report directly to the FA3 HF coordinator. Although I note that the HF coordinator reports to the technical director, it is not clear what level of influence the HF coordinator has overall.

376 For the UK EPR I understand that there is only one dedicated HF engineer. This is clearly insufficient for a project of this size and even if the FA3 HF engineers are claimed to be available for the UK EPR, I would still consider their team size insufficient. I further consider that this has contributed to the position that EDF and AREVA are in at the end of Step 4 with regard to HF.

377 EDF and AREVA claim that the engineers working on the project undergo training in HF. Chapter 18.1 of the PCSR (Ref. 17) states:

"*A training course in HF has been developed for the design engineers in the Engineering Business Units. The course lasts three days and is centred on design ergonomics and HFE at the design stage. It provides the engineers with some basic knowledge in this* *area, and enables them to understand the HF approach and to identify studies topics that require consideration of HF, since they affect future activity*."

378 Although I acknowledge that it only gives limited insights into the training of engineers, my review of the training materials (submitted in response to TQ-UKEPR-1354) suggests that, at best, it will provide an awareness of the importance of HF and key areas to be considered. It is highly unlikely to be able to equip design engineers to implement HF satisfactorily at a detailed design level.

379 I have found no evidence that EDF and AREVA operate a formal process for allocating HF resource or whether a SQEP HF person is required at design review meetings. The MCR appears to have been the main focus of HF attention for the project, based on the volume of HF documentation on this topic.

380 Unfortunately, this focus on the MCR may have had a detrimental effect on the HF consideration of non-MCR parts of the design (e.g. building, systems and equipment designs). Documentation detailing HF requirements is often very high level and not prescriptive enough to ensure compatibility across the facility design. It is quite possible that individually sub-contracted equipment could meet the design requirements, yet have coding and operational philosophies which are incompatible with each other.

381 My overall conclusions are that there has been inadequate HF SQEP resource (i.e. too few HF staff) to ensure satisfactory HF integration, and an over-reliance on design engineers addressing HF issues using HF guidance and requirements documentation.

> ***AF-UKEPR-HF-25 –*** *The licensee shall ensure that sufficient SQEP HF resource is identified and deployed to meet the demands of the on-going design and safety case work for the UK EPR.*

4.5.2.2 Technical Scope of Work

382 I assessed the HF and HF related technical activities undertaken at a very high level, as the quality and adequacy assessment are undertaken in detail via the other work streams in my assessment programme. My focus was on assessing the processes that EDF and AREVA have in place to deliver quality HF work and this is reported below.

Integration with the Plant Design

383 There is evidence of a considerable focus on the detailed design of the MCR HMI throughout the design development process, including operational experience inputs (see below), simulator studies (Refs 66, 68 and 69) and the HF evaluation programme to 1st Fuel Load (Ref. 61). The adequacy of the outcomes of some of these processes are assessed in more detail in Work Stream 5.

384 EDF and AREVA's HFI approach for the general design of the facility has been to provide HF requirements that have been integrated within the specification documents (buildings; systems and equipment levels). I consider this would potentially be an acceptable way of ensuring good HFI, if the HF content is adequate. However, based on my review of a selection of EDF and AREVA's supplied documentation, the quality of the integrated guidance is variable and often insufficiently prescriptive to be applicable by a designer (see Work Stream 3 assessment for further details). Consequently, I do not judge that this approach has sufficiently addressed detailed HF design requirements.

Definition of the User

385 The importance of understanding the user when designing complex multi-operator systems is recognised in British Standards (BS), International Standards Organisation

(ISO) and International Atomic Energy Agency (IAEA) standards. It is also recognised by the HFI TAG (Ref. 7) which states that "*The staffing concept for the system and an indication of their required capabilities and responsibilities (should be sought). This is also known as the 'target audience description*'".

386 Chapter 18.1 of the November 2009 PCSR (Ref. 17) makes no reference to any detailed Target Audience Descriptions or User Performance documents. However, it does mention "Future Users" in the various sections:

*"2.2.3.2. **Functional specification** - …A full-scale model of the Main Control Room is used to evaluate the proposed plan. Future users (represented by operators that manage existing plants) are involved in the evaluation, and the plan developed to best meet the demands of the activity.*

*2.3.2.2. **General operational management studies** - …The layout of the control room and auxiliary rooms was covered by a specific study including competencies in ergonomics and in architecture. The objective of this study was to design a control room and auxiliary rooms where the layout was tailored as closely as possible to the activities taking place there. The first stage consisted in identifying the factors governing the activity of the operating team in existing units and then defining the needs of future users (including operating disciplines not included in the operating team but working in liaison with it)."*

387 EDF and AREVA define the future user as existing French operators. I have sought a detailed user definition with associated anthropometric data, but only very limited details have been provided. No reference was made to any consideration of secular trends in the operating community with respect to physical size, age, sex, education, etc.

388 A failure to specify detailed anthropometric data could be mitigated by the use of CAD software, which incorporates detailed anthropometric modelling, such as SAMMIECAD. However, no evidence has been provided that indicates the use of such a system by EDF and AREVA. Discussion with EDF's representative during an inspection visit, claimed that they use a standard engineering CAD system and could take measurements from the drawings, but it was not common practice to do so, unless a specific issue was noted during a design review. This piecemeal approach leaves anthropometric issues to be picked up either during trials (a process that will only be successful if the end users represent the full percentile range of users) or during design reviews. My inspection of design review minutes supplied by EDF and AREVA has not found evidence that these aspects are considered comprehensively or systematically.

389 I conclude that EDF and AREVA have not adequately defined the 'user' for many aspects of the design. They particularly need to determine how future trends are likely to impact on the existing design requirements for both MCR and local plant operations (including maintenance).

> ***AF-UKEPR-HF-26 –*** *The licensee shall produce a user definition document that contains relevant anthropometric details and has considered the impact of secular trends in the operating community.*

Use of Operational Experience Feedback

390 EDF and AREVA have made considerable claims on its use of OEF as a key input to the UK EPR design. My review of supplied EDF and AREVA documentation has revealed no formalised process for the capture of OEF (i.e. the gathering, collation and use of OEF information). However, despite the apparent lack of a formal process, it is clear from the supplied documentation that EDF and AREVA have carried out a considerable amount of

OEF work in support of the EPR design. In fact, I consider it to be one of the main strengths of their HFI approach and does form a key input into the design. Many design changes appear to have been made over existing plants, which have resulted from OEF studies.

391 EDF and AREVA supplied a comprehensive list of OEF studies for both the MCR and general plant areas, although largely un-referenced. The MCR studies comprised the following four stages:

- Stage 1 (between 1996 and 1997) focussed on -
  - *"Equipment and resources available to operating personnel (video displays, communications, paper documents, computerised procedures etc.),*
  - *Workflow and task breakdown (content, sharing and interaction between tasks etc),*
  - *Physical environment (space, noise, light etc.),*
  - *Training (skills acquisition and maintenance)."*
- Stage 2 *"involved observations in the control room of Chooz B1, during unit-at-power testing. The following issues were specifically examined:*
  - *Plant overview panels,*
  - *Displays,*
  - *Operation log,*
  - *Analogue equipment assemblies (analogue recording graphs)."*
- Stage 3 *"of analysis involved observations in the control room of Chooz B1 from December 1997 to March 1998 during both at power and intermediate shutdown conditions. This was complemented by interviews at two other plants in order to gather additional information on the benefits (or otherwise) of computerising certain tools. The following issues were specifically examined in this third stage:*
  - *Benefits of computerising the analogue recording assemblies (analogue graphs) and the operation logs,*
  - *Benefits of computerising normal operating controls,*
  - *The way in which the HMI is used by shift managers and management staff."*
- *"The fourth stage of analysis involved observations in the control room of Unit 1 at Chooz B between October 1999 and December 1999, during the first unit outage. The following issues were specifically examined in this fourth stage:*
  - *Equipment and resources available to operating personnel (video displays, communications, paper documents, computerised procedures etc.) during unit outage,*
  - *Benefits of computerising normal operating controls,*
  - *Workflow and task breakdown (content, sharing and interaction between tasks etc)."*

392 I consider that the studies described appear to be reasonably comprehensive in their scope but, as these studies have not been supplied for assessment, I have not been able to determine their efficacy.

393 My Work Stream 3 assessment has examined operating experience inputs for non-MCR locations. Where studies have been supplied for review, for example, '*Summary and Results of the FA3 and 4 ETB Ergonomic Study*' ECEP060987 (Ref. 65) there is often very little detail on the methodology followed to generate the results.

394 Overall, it is apparent that EDF and AREVA have applied OE as a key element of their HFI approach. However, from the evidence provided, I have not been able to determine how this has fed into the design at a detailed level, or determine the total extent of its coverage.

Suitability of Standards and Guidance Used

395 I have conducted a review of the standards used in the EPR design - a summary of which is shown in Table 12 below. EDF and AREVA claim that they apply relevant international standards where these are available, sometimes via the equivalent French national standard. Internal EDF and AREVA standards are used where no other appropriate standards exist. Where a cited standard has been replaced, EDF and AREVA advise that they now use the current standard.

Table 12: Standards and Methods Applied to the UK EPR Human Factors Analysis Programme – standards review

Standard	Current?	Comment
International organization for standardization (ISO)		
ISO 13407: Human-centred design processes for interactive systems (1999).	N*	No longer current. Replaced by ISO 9241. *However, used in combination with other ISO and United States Nuclear Regulatory Commission (US NRC) standards, it is unlikely to prejudice the HFI process.
ISO 11064: Ergonomic design of control centres (2008).	Y*	Acceptable international standard. The standard is split into 7 parts which address all elements of Control Centre Design. *Although the standard is comprehensive, it needs to be considered alongside the requirements of the tasks being performed at the control rooms / areas.
ISO 9241: Ergonomics of human system interaction (2002).	Y	Current international standard.
ISO 80416: Basic principles for graphical symbols for use on equipment (2005).	Y*	Current international standard.
ISO 7000: Graphical for use on equipment (2004).	Y*	Current international standard. *As long as the symbols adopted for plant components match UK convention or are easily recognisable.

Table 12: Standards and Methods Applied to the UK EPR Human Factors Analysis Programme – standards review

Standard	Current?	Comment
ISO 14617: Graphical symbols for diagrams (2004).	Y*	Current international standard. *As long as the symbols adopted for plant components match UK convention or are easily recognisable.
ISO 13406: Ergonomic requirements for work on flat panel display screens.	N*	No longer current. Replaced by ISO 9241. *However, given that the panels used are likely to be Commercial Off The Shelf (COTS) equipment compliant with the latest standards and the HCI layout subject to strict user testing and V&V, I have no concerns with the use of this standard. EDF and AREVA also reference ISO 13407 which is the latest ISO standard for Displays and Controls.
ISO 15534: Ergonomic design for the safety of machinery (2000).	Y	Current international standard.
ISO 14738: Safety of machinery – anthropometric requirements for the design of workstations at machinery (2002).	Y*	Current international standard. *However, should be used in concert with ISO 13852 when considering reach / access issues associated with maintaining separation between user and hazard.
ISO 6385: Ergonomics principles in the design of work systems. (1990).	N*	Revised and updated in 2004 *However, other current HFI standards are quoted.
United States Nuclear Regulatory Commission		
NUREG-0711: Human Factors Engineering Program Review Model (2004).	Y	Acceptable USNRC standard providing detailed guidance on how to manage HFI. Comparable with UK approach.
NUREG-0700: Human-System Interface Design Review Guidelines (2002).	Y	US standard but internationally recognised.
International electro-technical commission (IEC)		
IEC 80416: Basic principles for graphical symbols for use on equipment (2002).	Y*	Current international standard. *As long as the symbols adopted for plant components match UK convention or are easily recognisable.
IEC 60073: Basic and safety principles for man-machine interfaces, marking and identification (2002).	Y	Current international standard. Considered appropriate with the caveat that the coding and markings based on this standard match UK NPP conventions.
IEC 60447: Man-machine interface – actuating principles; (2004).	Y	Current international standard.
IEC 60960: Functional design criteria for SPDS; (1988).	Y*	* Whilst still current, the publication date makes the content of this standard questionable given the advances in HCI.

Table 12: Standards and Methods Applied to the UK EPR Human Factors Analysis Programme – standards review

Standard	Current?	Comment
IEC 60964: Design for control rooms of nuclear power plants.	Y	Current international standard.
IEC 61227: NPPs – Control rooms – Operator controls.	Y	Current international standard.
IEC 61771: NPPs – MCR – Verification and validation.	Y	Current international standard.
IEC 61772: NPPs – MCR – Application of visual display units (1995).	Y	Current international standard.
IEC 62241: NPPs – MCR – Alarm functions and presentation.	Y*	Current international standard. * However, the following caveat applies. The UK has largely adopted the EEMUA guidance for alarm procurement and design.
Electric Power Research Institute		
EPRI: Human Factors Guidance for Control Room and Digital Human-System Interface. Design and Modification (2005).	Y	Current appropriate guidance.
Institute of Electrical and Electronic Engineers (IEEE)		
IEEE 1023: guide of application of human factors engineering to systems, equipment and facilities of nuclear power generating systems (1988).	N	Updated and re-issued in 2004.
French Norms (NF)		
NF EN 897-2: Sécurité des machines – Spécifications ergonomiques pour la conception des dispositifs de signalisation et des organes de service – Partie 2 : dispositifs de signalisation (1997), (§ 4 Dispositifs de signalisation). [Safety of machinery – Ergonomics requirements for design for means of signalling and components.]	Y	French national standard.
NF D 62-042: Mobilier de bureau. Tables et bureaux. Caractéristiques générales. Essais et spécifications. [Office furniture. Tables and desk. General characteristics. Tests and requirements.]	Y	French national standard.
NF D 62-041: Mobilier de bureau. Meubles de rangement. Caractéristiques générales. Essais et spécifications. [Office furniture. Storage unit. General characteristics. Tests and requirements.]	Y	French national standard.
NF EN 527-1, NF EN 527-3 : Tables de travail et bureau. [Table and desk.]	Y	French national standard.

Table 12: Standards and Methods Applied to the UK EPR Human Factors Analysis Programme – standards review

Standard	Current?	Comment
NF EN 1021 parties 1 et 2 : Evaluation de l'allumabilité des meubles rembourrés. [Test of capacity to take fire for stuffed furniture.]	Y	French national standard.
NF EN 1335-1, NF EN 1335-2 et NF EN 1335-3 sièges de travail de bureau. [Office chair.]	Y	French national standard.
NF EN 13761: Sièges visiteurs. [Visitors chair.]	Y	French national standard.
NF D 65-760: Armoires vestiaires rectangulaires métalliques. [Hanging cupboard.]	Y	French national standard.
AFNOR NF X35-102: conception ergonomique des espaces de travail en bureau. [Ergonomic design for the workspace in office.]	Y	French national standard.

396 I consider the standards applied generally constitute recognised good practice. In some instances the standards have been superseded, but in all cases the out of date standard is being used in concert with other in-date good practice standards. I judge this approach unlikely to prejudice the design of the EPR.

397 Whilst the declared standards are generally acceptable from a currency perspective, there is an issue with their scope. The standards applied are not comprehensive when considered in the context of whole plant design and are focused on the MCR. This raises a concern that the HFI process is not being applied effectively across the entire facility. Notable omissions are the lack of:

- A defined French or British anthropometric database.
- Maintenance / accessibility data (such as contained within UK defence standards).
- Defined general workspace (i.e. non control room) environmental standards.
- Computer based procedures good practice.
- Paper based procedures good practice.

***AF-UKEPR-HF-23 –** The licensee shall ensure that the system and equipment design specifications contain a detailed set of HF requirements and are based on recognised standards where appropriate.*

Operability Trials

398 EDF and AREVA place a strong emphasis on operability trials as a key part of the MCR HMI design development (see Refs 61, 67, 68, 69 and 70); hence I have considered their process in some detail.

399 I have not been able to identify a management document that describes EDF and AREVA's general methodology for the conduct of operability trials. However, they have supplied a suite of documents that describe in detail the conduct and history of some of the trials to date (Refs 37, 66, 67, 68, 69, and responses to TQ-UKEPR-769 and TQ-

UKEPR-1049). These references also mention a series of trials that were conducted in 2009, although I do not have a corresponding report for assessment.

400 A summary of EDF and AREVA's generic approach (based on the above references) for conducting operability trials is described below. This approach is largely in line with UK good practice, with some exceptions.

1. Define purpose of the test.
2. Define the test schedule.
3. Define material and human resources.
4. Define Scenarios / Topics for assessment.
5. Define data collection methods / metrics.
6. Define session protocol.

401 Although this approach appears generally sound, there are a number of additional areas where they do not appear to meet good practice in my judgment:

- There is no discussion on the effects that independent variables could have on the outcome of the trials.
- There is no discussion on how the data generated by the trials is actually analysed.
- The cognitive workload assessment method; Instantaneous Self Assessment (ISA) does not appear to have been validated or justified for use outside of its Air Traffic domain,
- There is no evidence of a consolidated issues / assumptions register being utilised (see below) for issues arising from trials.

Tracking and Resolving HF Issues and Assumptions

402 The requirement for a process for tracking and resolving HF issues comes from TAG T/AST/058 (Ref. 7) expectations for a HFIP which should include identification of:

"How assumptions, uncertainties and project issues and risks will be managed and resolved."

403 Compliance with this requirement in the UK is usually achieved through the use of an issues register, which is a database of issues that need to be addressed in the course of the design process. The main purpose of the HFI issues log is to outline the impact of each issue, prioritise them and propose a strategy for resolution. The HFI issues log should be a live document throughout the project.

404 I have not been able to identify a documented process for tracking and resolving HF issues. EDF and AREVA have recently introduced a HF Issues Register (HFIR) to capture issues arising from the human based safety claims substantiation work (see Work Stream 1). They have also described in the response to TQ-UKEPR-926, the process for tracking issues arising from MCR trials, but this does not provide sufficient detail to enable me to make a clear judgement on how well their process has been implemented.

405 I have been unable to identify any formal process for managing assumptions made during the design and analysis of the EPR design. There is a single claim in the document *Task Analysis Method Statement* (Ref. 42) that:

"*Assumptions made during the analysis will be recorded and substantiated at a later stage, when the required information becomes available.*"

406 However, no explanation is provided as to how this will be achieved.

407 Many reports do list assumptions, (e.g. Chapter 6 of the November 2009 PCSR) but do not attach unique reference numbers to facilitate tracking. The HRA Notebook (Ref. 29) allocate a unique code from A1 to A9 for tracking purposes, but there is no discussion as to what the process is/will be to verify and validate the assumptions.

408 I have not been able to determine how EDF and AREVA have tracked and resolved HF issues arising during the design process, or determine the adequacy of any trade-offs required in issue resolution. This lack of a consolidated issues and assumptions register is not consistent with my expectations.

409

410 ***AF-UKEPR-HF-27 –*** *The licensee shall establish and maintain a consolidated HF Issues Register for the future design and safety case development beyond PCSR. This will incorporate all outstanding HF Issues and requirements that have arisen from the work to the end of GDA.*

Management of Contractors

411 EDF and AREVA have not presented a formalised process for ensuring adequate HFI within contractor supplied equipment. However, they state that "*Specifications provided for supplier are written on the basis of the Human Factors approach described in the PCSR subchapter 18.1."* Additionally EDF and AREVA claim that all supplier designs undergo a rigorous validation process.

412 It is positive that EDF and AREVA specify general HF requirements, and these requirements may well lead to a design that is adequate in HF terms. However, in my judgment, they are not sufficiently detailed to ensure that the resultant design will be both ergonomically sound and integrated with other elements of the design.

413 EDF and AREVA have not provided details of their validation processes beyond the following statements:

"The Manufacturer shall test the ability of the operators to use HMI. In particular, the Manufacturer shall:

- *identify difficulties related to utilization of the equipments (HMI issues), make a report of those difficulties,*
- *figure out and integrate at design stage corrective solutions.*

In accordance to standard [20]3, EDF may propose and carry out operational tests in the Manufacturer's factory in order to ensure HMI meets EDF requirements. Hence, the Manufacturer shall inform EDF of the date of operational tests, at least 2 months in advance. Modifications to programs and HMI equipment (control desks, cameras…) performed after those tests are in the scope of supply of the Manufacturer.

The Manufacturer shall test the ability of the operators to use HMI. In accordance to standard [20], EDF may propose and carry out operational tests on site, in accordance with the Manufacturer, in order to ensure HMI meets EDF requirements.

Modifications to programs and HMI equipment (control desks, cameras…) performed after those tests are in the scope of supply of the Manufacturer."

414 The validation of supplier equipment is good practice, but it places the emphasis on testing to capture issues and cannot, in my judgment, replace the need for detailed guidance and standards for suppliers. For example, unless the supplier validation process considers the interactions between individual HMIs from different suppliers, it will not likely detect potentially dangerous transfer of training issues.

415 Another important mechanism for ensuring that outsourced equipment meets good HF practice, is the design review or independent peer review of supplier documentation. Unfortunately, although requested via a technical query (TQ-UKEPR-1026), the information was not available in time for my assessment.

416 My overall judgement is that there are areas for improvement relating to EDF and AREVA's control of contractors for the design HF. It currently relies on HF requirements in specifications provided and then on later validation testing. As discussed in my Work Stream 3 assessment and on my examination of their HFI scope, I judge EDF and AREVA's specifications are insufficient to ensure detailed designs that are optimised from a HF standpoint. I have recognised and addressed this issue via the Assessment Findings for Work Stream 3.

> ***AF-UKEPR-HF-22 –*** *The licensee shall ensure that the adequacy of HF maintenance and maintainability requirements is explicitly addressed in their V&V programme.*
>
> ***AF-UKEPR-HF-23 –*** *The licensee shall ensure that the system and equipment design specifications contain a detailed set of HF requirements and are based on recognised standards where appropriate.*

Integration with the Safety Case

417 I have not been able to find any evidence of integration between the HFE work encompassed by their HFI plan and the HRA undertaken in support of the PSA and safety case. I raised this as a concern at GDA Step 3. Discussions with EDF and AREVA have since revealed that such integration is not a requirement for the French regulatory approach for FA3, and no explicit integration had taken place until the recent task analyses of key human based safety claims (reported in Work Stream 1).

418 However, I note that there is a common basis for both the HFE programme and HRA work, in that it stems from the basic plant safety studies undertaken at the outset of the EPR project (see Chapter 3.1 of the PCSR). Additionally, the HFE programme has included significant fault scenarios within the design development trials to ensure that the MCR HMI supports emergency response operations.

419 I consider this lack of integration to be significant. however, I judge that the GDA Issue and actions that I have identified for Work Stream 1, namely the detailed substantiation of key claims for both pre and post- fault actions against the design, will ensure that a satisfactory level of integration is achieved for the PCSR stage.

420 It is my expectation that as the safety case progresses beyond the PCSR and into the PCmSR phase, a potential licensee should ensure that the HRA and HFE work are fully integrated.

> ***AF-UKEPR-HF-28 –*** *The licensee shall ensure that there is full integration between the remaining HFE programme, the HRA and the overall safety case.*

ALARP Process

421 I have not found any formal ALARP process relating to HF aspects of the design. This is not unsurprising due to ALARP being a particular UK requirement.

422 However, there is evidence of the application of relevant good practice, which supports the ALARP position for HF, including:

- The considerable use of operational experience.
- The use of relevant HF design standards.
- Detailed studies of current operations (e.g. Refs 45, 49, 50 and 65).

423 However , there are limitations in these areas, which I have discussed earlier.,

424 One of the other requirements of ALARP is the consideration of various design options to determine the 'best' solution in terms of risk and cost. My assessment has revealed little evidence of ALARP optioneering studies in the broadest sense, i.e. the use of traditional displays vs. task based displays, or SOA vs. Action on Receipt of Alarm.

> ***AF-UKEPR-HF-29 –*** *The licensee shall establish a process for addressing ALARP requirements for HF aspects of the design and safety case for the UK EPR.*

4.5.3 Conclusions

425 My assessment has been limited due to much of the evidence relating to HFI being submitted late in GDA Step 4, and some potentially important documents being provided in French. I have only been able to examine a small part of this material in detail however, in general, I judge that EDF and AREVA have undertaken a considerable HFE programme of work but that it falls well short of a satisfactory HFI programme for a project of this size. Key deficiencies are:

- A lack of integration with the HRA and safety case.
- Inadequately detailed HF design specifications; primarily for non-MCR designs.
- A lack of SQEP HF resource to support all design activities adequately.
- No overall HF issues project register.
- Excessive reliance on validation studies to ensure that systems and equipment designs match HF requirements rather than on detailed HF specification.

426 I found evidence that there has been a considerable HF design focus on the MCR HMI, which is potentially the most novel aspect of the overall design from a HF standpoint. However, I judge that there has been insufficient evidence of HF analyses for non MCR design development.

427 There has been considerable use of operational experience to identify HF requirements and improvements from existing plants. However, although I consider this a very useful input, it is not sufficient to ensure that the design reduces the risk from human error to ALARP.

428 Overall, there is little evidence of a fully integrated programme that actively works with other related technical disciplines in a cohesive manner to optimise the design and develop and iterate the safety analysis. In addition, although the major components of a recognisable HFI programme are evidenced, there are significant omissions.

429 I judge that the potential consequences of deficiencies of the EDF and AREVA HFI approach will be adequately addressed by the GDA Issue (**GI.UKEPR.HF1**) and the Assessment Findings I have identified from my Work Stream 3 and 4 assessments.

4.6 Work Stream 5: Plant-wide Generic Human Factors Assessment - Assessment

430 Chapter 18.1 of the November 2009 PCSR does not make any explicit claims relating to the goals of the HFE programme. A statement is made that *"The HFE programme helps to:*

- *Provide personnel with the resources they need for their work, so that they can achieve the required performance in terms of nuclear safety, quality, reliability and availability"*

431 Discrete claims are derived (not explicitly cited by EDF and AREVA as claims) in each of the Work Stream 5 assessment areas. This section explores the evidence relevant to the Work Stream 5 programme; the evidence is presented throughout the PCSR (and not confined to chapter 18.1) or has been derived through regulatory interaction.

4.6.1 Allocation of Function (AoF)

432 EDF and AREVA state in Chapter 18 of the November 2009 PCSR (Ref. 17) that *"The distribution of tasks between human operators and technical systems must be clearly defined to ensure that "the entity performing the operation" at a particular stage is clearly defined. The optimum distribution of functions between the human operator and the automatic control systems is achieved by taking account of the capabilities of the human operator and of the functions to be accomplished. This reflects the fact that the human operators and the automatic control systems do not have the same capabilities."* However, it should be noted that this is stated as a requirement rather than a claim as such. Therefore, I have assumed the implicit claim is that the requirement will be met.

433 The actual requirements for AoF are stated: "*Automatic control systems are allocated to repetitive tasks or those beyond the physiological, psychological or cognitive abilities of an operator (i.e. those involving very short response times or very large amounts of data etc). Such choices must also allow information relevant to the plant's operation to be acquired and maintained: thus enabling the operators to carry out operational actions themselves in all situations whether normal or abnormal: i.e. the design must support a high level of situation awareness"* (Ref. 17).

4.6.1.1 Allocation of Function Principles

434 The main principles stated to have been adopted by EDF and AREVA are as follows:

435 *"Tasks that require a rapid or very reliable response must necessarily be automated. They are:*

- *Operational actions required within 30 minutes of an accident in order to achieve a controlled state or a safe shutdown state;*
- *Actions required in the short term to prevent danger to personnel or irreversible degradation of equipment." (Ref. 17).*

4.6.1.2 Allocation of Function Method

436 The described process for determining AoF comprises four stages:

1. Definition of operational criteria; these are aspects of required tasks relevant to automation.

2. The designers suggest which operational actions should be automated, based on OEF taking account of the defined criteria.
3. Operational crews are asked to suggest which actions should be automated.
4. The designers analyse and review the proposals to make a final determination.

437 The November 2009 PCSR (Ref. 17) lists 13 criteria to be considered when undertaking AoF. For example: To meet workload demands: *“C1 Monotonous or repetitive tasks that, unless automated, would constitute an overload for the operators or are expected to lead to operator error through inattention and boredom.”* Or to manage actions required within a restricted timescale: *“C2 Actions on components required in very short timescales to keep the plant in operation”.* I consider this list of 13 criteria to be comprehensive and appropriate. In addition, it is qualified by the proviso that: *“Automation implementation must at all times leave the operators in charge of the installation, so that they can manage..”* both *“…the diversity and variability of the work situation that automatic devices cannot exhaustively cover”* and the *“possible failure of automatic devices, when take over by manual control is required”.* This is further emphasised in the definition of information to be presented to the operator, within which a key function is to indicate *“The status of automated functions (control loops, automatic sequences, protection mechanisms, etc.) and the way they interact with the process status”.*

438 The actual process of carrying out AoF for plant control elements is described in detail in Ref. 141. This is the basis for the procedure set out in the November 2009 PCSR (Ref. 17) and further qualifies the AoF process. It makes it clear that the basis of the automation in UK EPR is that applied in the N4 plants, and that the UK EPR is a development or evolution from these. Ref. 141 provides detail on the use of required operator action timescales to specify AoF.

439 For critical plant protection actions, i.e. on classified systems, AoF takes into account the time required by the operator to diagnose the event and decide on the required action. This diagnostic and decision time is then added to the estimated time for the action to be completed. This total time is then set against the process requirement. However, this process does not fully reflect the subtleties of human actions. The target time, ”T”, is the time from the first appearance of a significant indication in the MCR, to the time when lack of corrective action would result in *“significant aggravation”*, i.e. some nuclear consequences of the incident. The duration for diagnosis of the event ‘t’ is set at 15 minutes. The time to execute the required actions, ‘t”. is 15 minutes for control room actions and 45 minutes for local to plant actions. The rule is then: *“if T≤ t + t' then the action must be automated”*. This means that, in the case of an MCR action, if “T” is 30 minutes or less then the activation of the action must be automated. In the case of a local-to-plant action, then automation must be applied if “T” is less than 60 minutes.

440 In the case of unclassified systems, the estimated minimum time permitted for action, which must then be automated, is 10 minutes if resources are available in the MCR, 20 minutes if the actions are undertaken in the turbine hall or electrical rooms and 30 minutes elsewhere.

441 Ref. 141 explains that the AoF rules differ in terms of functional categorisation: for categorised functions (F1A, F1B, F2), principally, the time constraint rules are different from those for non-categorised functions. Each system is thus assigned an AoF based on the appropriate rules and taking into account the process and criteria described above. However, supplementary rules may also be applied which take precedence over these criteria, for example:

1. All initial start-up and shutdown sequences for major actuators shall be carried out by manual request.
2. The AoF should take account of the appropriate automation of the system in N4 plants and it should be checked by OEF that the automation has proved favourable.

442 It appears that a systematic process has been applied; this largely builds on the evolutionary aspects of the UK EPR. The criteria and the described scheme are in accordance with accepted practice in undertaking AoF. The scheme accounts for human skills and limitations, however my concern is that there may be too much emphasis on time available for action rather than an in-depth consideration of the required human attributes. Workload is considered in the criteria and there is clear consideration given to ensuring that the operators are fully aware of the automatic actions. There is an emphasis on ensuring that major activities are initiated by manual action and this is what I would expect.

4.6.1.3 Assessment of four Functional Allocations

443 There are no detailed task descriptions or analyses presented or referenced in the November 2009 PCSR (Ref. 17) with which to undertake functional allocation assessments. I therefore based my assessments on three of the task analyses developed by EDF and AREVA as part of their qualitative substantiation programme. In addition, I was able to witness a fault scenario simulation which enabled me to observe the automated features of the UK EPR in operation.

444 This lack of explicit AoF analyses has significantly limited my ability to make judgements in this area, therefore my views are based only on assessment and observation of resultant functional allocations via the task analyses and simulator observation.

<u>Starting the Standby Diesel Generators</u>

445 This scenario as described in Ref. 41 as *"the remote start of the Station Blackout (SBO) Diesel Generators (DG) following a Loss Of Offsite Power (LOOP) and failure of the Emergency Diesel Generators (EDG) to start"*. The scenario has two key components when considering AoF.

- Following a LOOP, the EDG should start automatically. The EDG are required to meet a LOOP and clearly this is an action required immediately. The operating team should be confident that the EDG are running when confronted by a LOOP and they should be supported by information that this action has occurred.
- If the EDG cannot be started then the SBO DG must be started manually.

446 The task analysis used a simulated scenario as its basis and this was limited by the facilities available in the current simulator. The SE and SS were not represented, so that all tasks were undertaken by the OS and the OA. The operators knew what to expect and were not distracted by the ancillary tasks to be expected in the MCR during such an event. On the other hand, the interface navigation facilities were not fully implemented hence operations were delayed to an extent.

447 In this scenario, the workload appears to be manageable although I note that ancillary tasks were not simulated, but then the SS and the SE were not represented in the MCR. The analysis demonstrated that the SBO DG can be started within the required grace time.

448 I consider in this case, that the SBO DG manual start is achieveable and that AoF is not be a prime factor in this scenario.

Automated Response to a Small Break LOCA

449 In this second scenario, the operating team must initiate cooldown from the MCR following a small break LOCA. However, the Medium Head Safety Injection (MHSI) is unavailable. A partial cooling is automatically initiated on the Safety Injection signal that initiates this fault scenario. The operators must then manually initiate cooldown when the automated partial cooling is complete (Ref. 42). The analysts calculated that, in this scenario as a bounding case, the operator response should be to start cooling within 30 minutes. This means that, in the event of this scenario, the operating team is restricted to the OS, OA and SS, as the SE is not planned to be available for 40 minutes from the onset of an accident scenario. In this event, the AD system is triggered and provides the principal cue that manual cooldown is required; it is not necessary for the operators to carry out any diagnosis, and the required actions are prescribed. If the operators make an error in the procedure, this will be revealed as the deteriorating plant parameters resulting from the error will lead to the AD detecting a changed situation. Nevertheless, this analysis concluded, on the basis of the simulator run, that the defined procedures could not guarantee that manual cooldown would be initiated within the 30 minutes.

450 In this scenario, the workload is apparently not manageable given the target time of 30 minutes. It may be the case that additional automation sequences could provide a solution, but the analysts suggest that the procedural sequence could be reordered and made more efficient. Therefore, this example does potentially highlight that the AoF process has identified this scenario as being problematic.

Cross-connection of the Emergency Feedwater Supplies

451 In this scenario, an unspecified external hazard has led to the requirement for the Emergency Feedwater System (EFWS) to be used to ensure heat removal by the SG (Ref. 43). However, the initial event has also caused a loss of the Essential Service Water, loss of the Component Cooling Water System (CCWS) and two EFWS trains are also unavailable. The AD system provides guidance to the operators with regard to the actions to be taken in response to the loss of CCWS. Two operator-initiated actions are required: firstly, cross-connection of the EFWS system which provides 24 hours water supply; and secondly, the operators are required to replenish the EFWS tanks from the fire-fighting supply to enable the EFWS to provide to the SG for 100 hours.

452 Clearly, this is a complex scenario with severe consequences, although I consider that the MCR operators will have sufficient cues to initiate the cross-connection. The MCR operators instruct a local-to-plant operator who carried out the required valve operations in the pump house. Although this is not an arduous task and one that can be initiated manually, I consider that in a serious transient it may be difficult to access the pump house and hence it may be preferable to enable remote operation of the crossover valves from the MCR.

453 In this scenario, the workload appears to be manageable although it was not possible to stage the full scenario in the simulator. The analysis demonstrated that there are no AoF issues other than the consideration of implementing remote operation of the EFWS crossover valves.

Steam Generator Tube Rupture (SGTR)

454 This scenario was demonstrated in the simulator although the primary purpose of the demonstration was not AoF. My focus was the crew performance and how they interacted with the process, and the way in which their activities integrated with the automated facilities. As this was a demonstration by the simulator staff, it was clear that the ‘crew’ knew which event to expect and were familiar with the scenario. Despite this

limitation, the demonstration enabled me to gain useful insights into many aspects of the interaction between the HMI, operator roles and procedures.

455 My focus from an AoF perspective was the reliance placed by the operators on the AD and whether the activation of the AD could lead to operators losing their situational awareness, and hence their overview of the process, as they negotiated the failure procedures. I understand that there is a degree of automated response to an SGTR and my observations confirmed that both OA and OS were not rushed in their actions. The SS requested certain displays to be placed on the POP at the start of the scenario which aided monitoring of the situation.

456 In order to challenge the AD system, I requested the OA to make a deliberate operational error by isolating a non-failed steam generator. The automatic procedures continually reminded the operator that the strategy was not having the expected effect of improving plant condition. Eventually the signals from the AD could not be ignored and the team recovered the situation by following the recommended actions and then proceeded to isolate the faulty steam generator.

457 Workload was not an issue in this scenario, and even with deliberate errors the various operations were undertaken in a timely manner. In my opinion, there was no evidence in this scenario that the AoF process was inadequate.

4.6.1.4 Conclusions

458 I have not been able to undertake a complete assessment of EDF and AREVA’s AoF analyses. From the limited assessment I have been able to undertake, I judge that the method and criteria applied appear sound. I have only been able to consider resultant functional allocations via the limited task analyses developed for GDA Step 4. This has significantly limited the judgements that I am able to make and the conclusions that I am able to draw in terms of the adequacy of the AoF on the UK EPR. However, from the limited material considered, it appears that the AoF decisions are largely adequate. I consider that further justification is required of the AoF for the UK EPR and that this be built into EDF and AREVA’s forward programme of task analyses. GDA Issue **GI-UKEPR-HF-01** in Annex 2 provides details of the requirements of this forward programme. AoF considerations are a key element in the necessary substantiation of human based safety claims.

4.6.2 Workstation and Workplace Design

459 These findings relate to item (2) from the methodology and scope presented in Section 3.2.9.

4.6.2.1 Anthropometric Data

460 Typically the PCSR would require that workspace components and workstations would be designed to accommodate a specific, relevant population range (e.g. 95th percentile males to 5th percentile females). There is a statement on anthropometric considerations in Ref. 142, which provides a table of the considered dimensions of the user population. I note that the EDF and AREVA data are “...*values for the French population. These values, which are the result of studies carried out prior to publication (1982) produce a document that is no longer up to date as the height of individuals is changing a lot*”. Whilst this is not ideal, the dimensions are broadly similar to those contained within the recognised anthropometric design “standard” for UK populations.

461 I also note that the application of anthropometric data does not account for the impact of growth trends on the physical dimensions of potential user populations. Over time, there is a change in some human dimensions known as the secular trend. Figures for stature change in the UK can be found in Ref. 143, which suggests that the trend is currently 10mm increase per decade in the working population. Furthermore, dimensions cited in "standards" are typically taken from sources that are sometimes several years old. For example, much of the data presented in Ref. 85 was obtained in the mid-eighties and hence by the time a UK EPR is commissioned, some of the data could be over 30 years old. It must be noted that this does not only affect estimates of length but obesity trends will also impact the space requirements for personnel in future facilities.

462 I therefore consider that the workstations should be designed to meet the current user population, based upon reasonable estimates of the secular trend.

> ***AF-UKEPR-HF-30 –*** *The licensee shall design the UK EPR workstations to accommodate the UK user population, based upon reasonable estimates of the secular trend. The anthropometric data applied shall be justified.*

4.6.2.2 Physical Arrangement of Workspaces

463 There are no specific claims relating to the physical design of workstations in Chapter 18.1 of the November 2009 PCSR (Ref. 17). The PCSR makes reference to "reviews" of the workspace layout of the MCR and its annexes. It is stated that *"The objective of these reviews is to achieve a design for the control room and its annexes that are as well suited as possible to the activities that take place in them."* Additionally, Figure 1 of PCSR Chapter 18.1 (reproduced as Figure 3 above) provides an overview of the EDF and AREVA's approach. However, only very limited information is given on the detailed approach to the workplace design in the PCSR and submissions provided.

464 Chapter 7 of the November 2009 PCSR (Ref. 17) states that "*The layout of the MCR and other HMI rooms has to respect the basic arrangement requirements for information presentation on both computerised workstations and hardwired control panels. Visibility, accessibility, communication between the operating staff members during all plant states have to be considered*" and "*The detailed layout will be developed, starting from the draft layout proposed, in a design process involving design staff, human factors specialists, and utility representatives.*" I take these to be EDF and AREVA's intentions for the EPR design.

465 However, there is no specific evidence presented in the PCSR for the physical layout of the control room and wider plant workspaces. Therefore my judgements in this area are purely high level opinions based on visits to the FA3 simulator, and I highlight that I did not undertake measurements of the physical design of the FA3 simulator due to the fact that it is not necessarily applicable to the UK EPR.

466 In my opinion, the MCR layout is spacious and I consider that it could afford good visibility and accessibility throughout.

467 The PICS workstations are essentially office type equipment with contemporary desks and standard flat screen displays. Control is via mice and keyboards which are moveable on the desk surfaces. There is ample desk space for the lay-down of documentation. No screen adjustment facilities will be provided due to seismic considerations. No detail on seating is described in the PCSR (Ref. 17). However, it was observed in the simulator that normal office seating with adjustable facilities was provided.

468 The Plant Overview Panel (POP) appears visible from all working positions, although I note that the projection technology will differ in the UK EPR MCR. The layout of the SICS was represented by a static paper mock-up in the simulator. The layout of the SICS panel is designed for standing operation and subjectively it appeared largely adequate in terms of visibility and reach.

469 I witnessed a demonstration of the three dimensional model of the plant which I am informed is used by designers to check and refine the design of non MCR areas. Standard proformae are used with the three dimensional model to check the general working environment at each piece of equipment, and these include access for maintenance. This process is not discussed in the PCSR (Ref. 17) however, EDF and AREVA advise that documents submitted in response to TQ-UKEPR-1026 illustrate the approaches taken. Unfortunately, these submissions were received too late to be included in my Assessment Finding.

> ***AF-UKEPR-HF-31 –*** *The licensee shall provide justification and evidence of the suitability of the workspaces and working positions in the UK EPR (not limited to the MCR) for the UK working population.*

4.6.3 Environment

4.6.3.1 Lighting

470 The principal claim made with regard to lighting in Chapter 18.1 of the November 2009 PCSR (Ref. 17) is *"The lighting in the MCR will provide optimal working conditions for the operations team."*

471 There are also additional statements related to lighting design presented in Chapter 9.5 of the PCSR including:

- *"Providing a lighting level suitable for the operational tasks (good contrast so that the information required may be read easily).*
- *Minimising glare and reflections.*
- *Each area within the MCR will have lighting appropriate to its particular function. This lighting will be adjustable, so the operators have adequate lighting for their tasks.*
- *Comprehensive arrangements are in force to ensure that lighting in the MCR, RSS and TSC is backed up by at least two trains. An emergency uninterruptible power supply (accumulator batteries) guarantees a minimum lighting level.*
- *Lighting in the MCR and TSC is also backed-up by the power sources provided for managing severe accidents."*

472 Further requirements are cited in Ref. 144 including the lighting levels, the choice and location of luminaires, the colour temperature of lighting and the uniformity of lighting. I have no significant issues with the requirements presented; the lighting levels are acceptable and correspond with relevant good practice in this area, However, Ref. 144 does not include all aspects of relevance, particularly relating to the detailed design of the emergency lighting system and the specification of minimum lighting levels in access corridors. EDF and AREVA indicate that these aspects are covered in submissions in response to TQ-UKEPR-1026 which were received too late for me to include in my assessment.

473 Chapter 18.1 of the November 2009 PCSR states that states that "…*batteries guarantee minimum lighting level*", and Chapter 9.5, (Ref. 17) states that the diesel generators will

provide two thirds of the lighting for the MCR and RSS, and that, in the event of their failure, the back-up diesel generators and batteries will provide one third of the lighting in the MCR.

474 I consider that the two thirds level provided by the diesel generators in the MCR and RSS is acceptable, though I am less assured by the one third level. However, I note that the one third level will only occur in infrequent scenarios following loss of off-site power and failure of all four emergency diesel generators. The PICS screens and the POP will remain legible as these are self illuminated, although I am unsure about the legibility of the SICS panel under such lighting conditions.

> ***AF-UKEPR-HF-32 –*** *The licensee shall provide further information on and justification relating to the emergency lighting design and relevant plant-wide minimum lighting levels.*

4.6.3.2 Heating and Ventilation

475 There are no explicit claims regarding heating and ventilation in Chapter 18.1 of the November 2009 PCSR (Ref. 17) although a comment is made that these issues are considered in the HFE programme.

476 Chapter 18.1 points to Chapter 9 of the PCSR for information relating to environmental conditions and additional information is presented in two of the references for Chapter 18.1. Chapter 9.4 of the PCSR presents the broad temperature ranges for areas within the plant. I have no significant issues relating to the ranges, although I note that prolonged exposure to a temperature of 26^{o}C in the MCR may induce drowsiness. In addition, the RSS has a maximum intended temperature requirement of 30^{o}C (but could be up to 40^{o}C under “exceptional conditions”) and I consider this to be too high as the RSS is likely to be occupied for prolonged periods. I consider its environment should be analogous to that of the MCR.

477 Information is provided in Ref. 142 regarding temperatures, air movement and humidity requirements for the simulator, which I have presumed will be required for the MCR and hence are incorporated into the system design manuals. These values generally correspond to recognised good practice, however I note that should the air conditioning system fail, the MCR temperature may reach 32^{o}C, which is in excess of the stated 30^{o}C 24 hour maximum for the MCR.

478 Chapter 9.8 of the PCSR also provides information relating to the design of the air conditioning systems for the MCR. I have no issues with the cited requirements in this regard as they reflect recognised good practice.

> ***AF-UKEPR-HF-33 –*** *The licensee shall undertake detailed analysis of the thermal environment in the MCR and RSS and provide justification of its applicability for the full range of conditions envisaged for operations from each location.*

4.6.3.3 Noise

479 Chapter 18.1 of the November 2009 PCSR (Ref. 17) addresses the issue of noise levels in the UK EPR. It claims, in Section 4.2.2, that: *“The acoustic environment and the main sound level in the MCR and the RSS are specified so that:*

- *The process monitoring and control and associated activities may be carried out in comfort;*

- *Good communication is ensured between members of the operations team, and*
- *Auditory signals are heard clearly.*

480 *This requires a sufficiently low average background sound level, good reverberation properties in the MCR, and appropriate sound level for auditory signals."*

481 Chapter 18.1 (Ref. 17) Section 4.2.2 summarises the engineering approach to ensuring that the MCR is isolated from machinery noise. In Ref. 142, Technical Specifications for the EPR Simulator, Section 5.3.3 provides a table which states that the design should aim to achieve less than 50dB(A) in the MCR and less than 55dB(A) in the RSS. A target reverberation time is cited as between 0.3 and 0.8 seconds. Ref. 142, Section 1.1 provides a comprehensive list of standards and regulations relevant to noise in the workplace. Section 4.3 defines the various objectives and constraints on noise which have led to the design targets.

482 Although little detail is provided within Chapter 18.1 of the November 2009 PCSR, (Ref. 17) I consider that the subsidiary documentation provides assurance that workplace noise is considered systematically within the UK EPR design. The evidence relates principally to the MCR and associated work places. I consider the declared targets for the MCR and RSS to be acceptable. 50-55dB(A) is considered representative of a typical working office environment (see for example Kroemer and Grandjean Ref. 145) and permits normal conversation to be conducted (NUREG 0700, Ref. 146). However, whilst the targets for noise levels and attenuation appear appropriate, the achievement of these targets will require verification.

> ***AF-UKEPR-HF-34 –*** *The licensee shall verify that the target noise levels have been met as part of the V&V of the UK EPR.*

4.6.4 Control / Display Interfaces and Alarms

483 The detailed design of the UK EPR interfaces is out of scope for GDA as they will not be developed until GDA Phase 2. Therefore, I have considered the proposed interface designs for the FA3 plant at a generic level against good practice in the area. I accept that the development the UK EPR interfaces is a significant task and much more than a simple translation issue. As a result, the final interface designs for the UK EPR may be somewhat different to those assessed here. However, the quality of the interfaces is an implicit assumption underpinning the HRA and it is on this basis that I have assessed their adequacy.

484 The November 2009 PCSR (Ref. 17) generally restricts description of HMIs to those provided in the MCR. Therefore, I have only considered the controls and displays provided within the MCR. However, where PICS displays are provided in the TSC and the RSS, then the observations made in this assessment also apply to those locations. No assessment has been made of HMIs that may be provided outside the MCR for the local control of plant systems as no information has been provided in this respect.

485 The interfaces have been developed in detail for FA3 and there are no English versions available. Therefore, my assessment was based on the interfaces described in the November 2009 PCSR and the associated documentation, along with my observations from visits to the simulator facility. As the interfaces are in French, my assessment is limited to the demonstration of the interfaces and their description, rather than a detailed analysis of individual display screens.

AF-UKEPR-HF-35 – *The licensee shall produce the detailed designs and justification of the human machine interfaces for the UK EPR.*

486 The main claim for the control and display interfaces is cited in the Instrumentation and Control System Chapter 7.1 of the PCSR, (Ref. 17):

487 *"All the means necessary to control and monitor the plant in normal operation (within specified operating limits and conditions) must be available to operators in the Main Control Room.*

488 *In addition, the operators must have at their disposal in the Main Control Room all the operating facilities required to carry out all actions claimed in the safety case.*

489 *If the Main Control Room is unavailable (due to a fire for example), the operators must be able to carry out monitoring and control of the plant from a Remote Shutdown Station, to allow a safe shutdown state to be reached and maintained."*

490 I note that this claim relates to equipment availability and does not prescribe human factors considerations to facilitate reliable human interaction.

491 The general arrangement of the MCR is shown in Figure 4. It comprises the following interfaces:

- Four PICS workstations – for normal and fault operations. These are replicated at stations for the OS, OA and SS, plus one additional unused.
- POP - Overview displays.
- Subsidiary PICS workstation - this is a reduced functionality workstation for use by non-operational staff – it can access PICS information but has no control functions. Not assessed.
- Conventional Control Panel – situated between the OA and OS work stations.
- SICS – Extended panels of conventional instrumentation for independent and diverse monitoring of plant status during out of normal conditions and for controlling the plant in the event of PICS failure.
- Fire Panel – not assessed.
- Maintenance work station – not assessed.

Figure 4: Diagram of proposed FA3 and UK EPR MCR

[redacted]

4.6.4.1 HMI Design Status

492 The general design of the HMIs for the UK EPR is derived principally as an evolution from the N4 plants and associated OEF. There is no evidence that the results from fault studies have been implemented within the HMI design. Current task analyses, being undertaken as justification for the claims for human actions, have revealed potential discrepancies in the availability of information to prompt operators to certain faults (see Section 4.2.2 on long term monitoring of actions required to maintain EFWS inventory).

493 The approach to the FA3 display design is summarised in Chapter 7 of the November 2009 PCSR, although further detail is specified in Ref. 147, which "*presents the principles retained for the design of operations displays on the EPR computerized HMI*", and also includes the "*work in hand*" on the "*Graphic House Style Book and Graphic Library*". This document provides the specification for the design of PICS displays and controls. In addition, the response to TQ-UKEPR-1085 regarding differences between the FA3 simulator and the UK EPR, included a document (Ref. 148) which provides valuable, additional information regarding the design of PICS displays, navigation facilities and the operation of the controls.

4.6.4.2 PICS workstations

494 Each of the four PICS workstations comprise five flat display screens that are controlled using one keyboard and mouse for all interactions. Any display format can be accessed at any workstation screen and formats can be directed to any other screen in the MCR, including any of the plant overview panel (POP) screens. There is an additional display screen that is not part of the PICS, which is separately used for administrative functions. As this is not related to matters of nuclear safety, it has not been assessed.

495 Typically, only the two front PICS workstations are used to control plant equipment. The other two workstations are locked out from control and only available for monitoring use, typically by the Supervisor. In the event of a workstation failure, control facilities can be activated on either of the rear work stations. However, only two work stations can be set to operating plant status at any given time, and this status is under supervisor control and requires authorisation by password. Further details of the PICS are provided at Annex 6.

496 Ref. 149 provides an account of a task analytical approach for developing the structure and content of the PICS formats. This combines a high level task description with generic information requirements and then tabulates the facilities required. Although this is a systematic process that generates specification requirements for control and information displays, it is not clear how it is used to develop actual page layouts.

497 There is no apparent link from the safety case fault studies to format design. There is no indication that any formal consideration of the identified faults, as listed in Appendix 7A of the November 2009 PCSR (Ref. 17), has been applied in HMI design. The task analyses which have been carried out recently (Refs 40, 42 and 43) do suggest that there is merit in considering how the interface is claimed in these scenarios.

498 No detailed 'style guide' for the design of the current PICS displays was provided in time for my assessment, although Ref. 147 (Display Specification) does provide high level requirements. A detailed 'style guide' is necessary to ensure consistency of design between different applications and to provide a complete and coherent demonstration of the treatment of HF in the design. This should be developed for the design of the UK interfaces. Such a style guide will provide assurance that coding conventions, particularly the use of colour and graphic icons, are used consistently and clearly. Moreover, it should demonstrate that these comply with the expectations of a British population. It should also provide guidance for arranging information on the screens in terms of system demarcation, association of related equipment items and the general density of information.

> ***AF-UKEPR-HF-36 –*** *The licensee shall provide a HMI style guide (or equivalent); using recognised modern standards to guide detailed design and justification of the interfaces and displays for the UK EPR.*

499 There are no permanent displays, for example an alarm list or general plant status overview, other than a permanent alarm header that does give information on the numbers and types of alarms. This should be reconsidered for the UK design, as typically fixed displays can support situation awareness and response to emerging issues. Any such overview could feasibly occupy a fixed area of the POP or be located on one of the OS or OA local displays. I consider this further in my consideration of the POP below.

500 The PICS provides a comprehensive array of navigation features which enable the operator to access information effectively. Features are provided within the displays to provide an awareness of the status of automatic actions. Furthermore, the interface does not typically require complex cognitive activities such as calculation or diagnosis, and the display structure and control plaques do not make excessive demands on memory.

501 EDF and AREVA have presented little information on ways in which PICS may partially degrade and how the operators will detect this and respond to such situations. I note that there is a 'life-sign' that is intended to give operators information on the health of the PICS functioning.

> ***AF-UKEPR-HF-37 –*** *The licensee shall ensure that PICS functional degradation is alerted to the operators.*

502 I note a number of minor ergonomics issues that should be addressed for the UK EPR HMI design. I consider that the character size may be too small for the expected viewing distances. I also observed apparent inconsistencies in the representation of mouse sensitive areas and in the operations for menu selection, along with a lack of an effective contrast ratio in the use of colour, particularly in the use of 'white', to indicate auto/manual status.

503 However, I note that these issues have already been noted by EDF and AREVA during simulation verification exercises, and that they will be further evaluated and resolved before implementation in the final design, **AF-UKEPR-HF-37** refers.

4.6.4.3 Plant Overview Panel (POP)

504 In the November 2009 PCSR, Chapter 18 (Ref. 17), EDF and AREVA declare *"One of the operators' key tasks is to monitor the plant status and check that all the essential systems are functional, so that corrective action can be taken if necessary. This requires having an overview of the status of the plant and its systems"*. The PCSR suggests that this requirement is limited by the smaller screens used for PICS information display and the limited array of information. EDF and AREVA have therefore designed an overview display format ('*tour de bloc'*) to support plant status overview monitoring during normal operations, and the SOA overview display during post fault operations.

505 A description of the POP is provided in Annex 6.

506 The POP is not claimed to support post-fault operations; it is designed primarily as an aid to normal operations to support team co-ordination and discussion. Currently, there are no dedicated formats for display on the POP; it allows any PICS format to be presented on the screen at the discretion of the OS and OA. I consider that a suite of dedicated formats for the POP would be beneficial in supporting operator situation awareness and reliability, and that this should be an option for the UK EPR.

> ***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.*

507 Anecdotally and from my own observations in the simulator; the POP appears visible from all MCR workstations. However, this has not been confirmed by analysis, and although the results of evaluation trials in the FA3 simulator will assist, specific confirmation will be required for the UK EPR.

> ***AF-UKEPR-HF-39 –*** *The licensee shall provide a justification and evidence of the visibility of the detailed POP displays proposed for the UK EPR.*

4.6.4.4 Conventional Instrumentation Panels

508 Two conventional, hard-wired panels are proposed for the MCR: a hard-wired panel at the OS/OA workstations and the SICS.

Hard-wired Panel at the OS/OA Workstations

509 A small console of conventional keys/buttons is proposed for the desk in between the OS and OA workstations. These are for the manual initiation of the reactor trip and turbine trip. The console will also include controls for the Public Address and other communications systems.

510 The positioning of these necessary controls is convenient for the operators although no details have been presented on the nature of the controls.

> ***AF-UKEPR-HF-40 –*** *The licensee shall justify the design of the hard wired OS/OA panels for the UK EPR.*

SICS Panels

511 SICS is an independent control system designed to provide control of the plant in the event of failure of PICS. It comprises a suite of three consoles equipped with indicators, alarm annunciators and conventional controls (switches/buttons) and is located in a corner of the MCR. The SICS panels are built up using modular instruments and is laid out in an array corresponding to the main plant systems. SICS is described in the PCSR (Ref. 17 (Chapters 7 and 18)) and with supplementary information in two further documents; Refs 149 and 150.

512 The November 2009 PCSR, Ref. 17 Chapter 18 states:

513 *"The MCS [SICS] is a conventional control and monitoring facility with a panel display containing buttons, indicator lights, alarm windows and registers, etc. The operator can carry out the following functions from the MCS [SICS]:*

- *Monitor and manage the station in a stable power state if the MCP [PICS] is not available for a limited short period under normal conditions,*
- *Shutdown and maintain the plant in a safe state, if the MCP [PICS] is unavailable for longer period under normal conditions,*
- *Monitor and implement appropriate operational management functions following accidents, so that the plant is brought to and maintained in a safe state when the MCP [PICS] is not available in a situation defined as PCC-2 to PCC-4, and*
- *Initiate measures to fight fires in the nuclear island when the MCP [PICS] is not available, for PCC-2 to PCC-4 events"*

514 Furthermore, the November 2009 PCSR claims, *"The SICS is designed so that it integrates the controls and information in a way that is optimal from an ergonomics perspective – the operators have no need to refer to other information sources to obtain the information they need for the task".*

515 Details on the operation of the SICS are provided in Annex 6.

516 My assessments of the SICS panels are based on the available documentation and consideration during visits to the EPR simulator, although it should be noted that the representation of the SICS in the simulator during GDA Step 4 was only a paper mock-up.

517 The panels appear well laid out with good segmentation between plant areas. The controls are generally within the reach of the operators, although this should be confirmed for the size range of potential operators.

518 I note minor issues regarding the legibility of the SICS labels and alarm legends, particularly at the rear of the panel. In addition, the displays presented on the small modular tiles may be difficult to view. However, I accept that this may be a function of the rendition of information on the mock-up.

> ***AF-UKEPR-HF-41 –*** *The licensee shall undertake detailed design and justification of the SICS panel for the UK EPR.*

4.6.4.5 Ancillary Control Rooms

519 Two ancillary control centres for UK EPR are considered in the November 2009 PCSR (Ref. 17); the Remote Shutdown Station (RSS) and the Technical Support Centre (TSC).

RSS

520 In the event that the MCR becomes uninhabitable, the operators trip the plant and move to the RSS. It is assumed in the PCSR (Ref. 17) that this takes a maximum of 30 minutes. There is little detail presented on the physical arrangement of the RSS, although it is stated that there will be two work PICS workstations. No POP or SICS is provided. My findings regarding to the PICS therefore apply.

521 The November 2009 PCSR states *"The decision criteria and arrangements for evacuation of the MCR and transfer to the RSS must be effective and ensure that effective control of all the necessary functions can be transferred."* Although I expect that the PICS workstations will support the limited activities necessary from the RSS, I consider that this claim is not sufficiently justified. Analysis should be undertaken to confirm that all required operations from the RSS can be achieved using the proposed control and display facilities.

> ***AF-UKEPR-HF-42 –****The licensee shall undertake detailed analysis and justification of the implementation of the PICS in the RSS to ensure that all required operations can be achieved.*

Technical Support Centre (TSC)

522 For additional supervision and support during severe accidents and some emergencies there is a TSC. No detailed information is provided about the TSC. However, EDF and AREVA propose that the TSC will be equipped with PICS workstations similar to those provided in the MCR, hence my findings relating to PICS apply.

4.6.4.6 Alarms

523 The EDF and AREVA claims for the alarm system are set out by the November 2009 PCSR in Chapter 18 (particularly Section 3.3) and Chapter 7 (particularly, Appendix C, Section 1.4.1) of Ref. 17. The declared functions and general form are described:

- *"An alarm is an alert message delivered by the instrumentation and control system to the operators warning them of an anomaly in the plant's operation or status. It requests them to take the appropriate action to manage the situation.*
- *The alarms are the binary signals that indicate faults in processes or equipment: audible and visual signals that attract the operators' attention when an alarm occurs and guide them towards the alarm sheet for the faulty equipment item or process.*
- *Alarms may be generated when process variables exceed their normal operating values, when an equipment item is not operating in a mode consistent with its current function in the plant, or when an equipment item fails." (Ref. 17).*

524 On detecting an alarm, it is said that the system will support operations as follows: "*The operations team manage the alarm (after it has been detected and identified) and:*

- *take corrective operational action;*
- *monitor the correct operation of an automatic process triggered by the anomaly;*
- *ask the relevant technical service to take action;*

- *monitor the development of the anomaly;*
- *apply the technical measures defined for the operational circumstances; and*
- *configure the plant as requested by the network manager to maintain or achieve a balance between production, distribution and consumption."* (Ref. 17)

525 The PCSR stresses that the alarm system must not overload the operator "… *with multiple alarms requiring simultaneous responses…"* It also requires that the guidance provided by alarm management must:

- *"indicate the relevance of the event to safety (does it require the routines used during accidents? Is action required to reinstate system safety?),*
- *indicate the severity of the event (is a function lost or degraded; or is its impact only minor?). The operators use a scale of severity set at the design stage to decide on the urgency of the alarm,*
- *take into account the plant state, so that an alarm is only raised if the plant's current situation requires it,*
- *reduce redundant alarms where multiple systems signal the same event,*
- *provide alarms with little synthesis, so that they are easy for the operators to interpret,*
- *suppress an alarm if one of higher priority occurs for the same function or equipment item."* (Ref. 17).

526 Details on the alarm system interface and its functionality are provided at Annex 6.

Alarm Philosophy and Design

527 The November 2009 PCSR lists a reference titled "*Principles for specifying and handling alarms for EPR*" (Ref. 151). This was supplied in response to a TQ and late in my assessment process, hence I have not been able to consider it for Step 4.

528 In general, I consider that the alarm system design largely meets accepted good practice and modern standards, is well integrated within the overall HMI concept and is consistent with the operating philosophy described in the PCSR (Ref. 17).

529 An alarm system should be effective in gaining the operator's attention without being distracting. I consider that the audible signals as demonstrated to me in the simulator facility are clear and distinctive, and the provision for silencing by the responsible operator potentially minimises auditory distraction during an incident, although this requires confirmation.

> ***AF-UKEPR-HF-43 –*** *The licensee shall justify the design of the audible alarm signals for the UK EPR.*

530 I consider that the visual alarm information is effectively presented and it is appropriate that it is displayed at the same position in the header on all PICS formats. I have no issue with the use of flashing and its timing. I consider the flash together with the change to alarm colour (depending on priority) provides satisfactory visual alerting cues.

531 The alarm messages are clearly presented in the alarm list and the *"Alarm Sheet"* provides effective guidance and supplementary support as the operator deals with the alarm and undertakes any remedial action. I note that the alarms are clearly prioritised by colour and alarm information is set out in a clear structure.

Alarm Configuration

532 The alarms are clearly prioritised within the system and the operation of the system is straightforward. The prioritisation is presented by the PICS interface and is consistently presented on the SICS. Configuration and coding is consistent within other interfaces such as the RSS and TSC as they apply PICS. There is no information on alarms relating to local to plant interfaces.

> ***AF-UKEPR-HF-44 –*** *The licensee shall demonstrate that a consistent approach to alarm prioritisation and configuration is taken throughout the UK EPR.*

Alarm Procedures

533 Each action on receipt of an alarm is specified in detail on an alarm sheet, which occupies one screen page of information. The operator can retrieve this alarm sheet with a single click from the main alarm list. The list provides information about the alarm and the procedure for dealing with its occurrence. The information includes direct buttons to access the appropriate operational displays to implement remedial actions. This is a powerful aid to operators as it provides immediate direction on the required actions in the event of any PICS alarm.

Alarm Flooding

534 Alarm flooding is a known contributor to human error. The PICS aims to mitigate this via:

- Prioritisation: The alarms are prioritised in four levels and the interface enables the inspection of active alarms at any priority level separately.
- Filtering: Filtering is based on conditioning by plant mode. This effectively reduces the number of active alarms displayed and highlights exceptional alarms relative to current mode. The interface displays the number of active alarms removed from the list and the operator can readily reveal the full, unfiltered alarm list if required. I consider this to be to be an effective aid in highlighting exceptional alarms and reducing the total of active alarms displayed.
- When a parameter returns to a normal condition, or is no longer applicable due to changes in the plant situation, the related alarm clears automatically, hence the list is not cluttered with unnecessary alarms.
- AD activation: In an incident when the AD activates, the operators are instructed to ignore the alarm display and the alarm audible signals (but not the AD) may be muted. In this situation the operators follow the SOA actions as directed by the AD.

535 I consider that these features will limit the potential for alarm flooding, however I note that no numerical targets for a maximum rate of alarm activation are defined in the system description. Although there is no requirement to respond to alarms directly once SOA procedures are entered, it would seem prudent to ensure that alarm flooding does not occur for abnormal and emergency situations.

> ***AF-UKEPR-HF-45*** *– The licensee shall set a maximum rate of alarm activation in the UK EPR alarm design specification.*

536 Although there is an alarm status indication on every PICS format, there is no permanent display of active alarms in the MCR. In order to support situational awareness, a permanent display of current alarms should be considered.

> ***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.*

537 The SICS panels present around 250 alarms (Ref. 149) as matrices of trans-illuminated annunciator tiles. The matrices are located on the upper area of the panels. I have not been able to assess the alarm design on the SICS panels, as the only information available (Ref. 149) refers to the sounds associated with SICS alarms. There is no information on the nature of the audible proposed.

> ***AF-UKEPR-HF-43*** *– The licensee shall justify the design of the audible alarm signals for the UK EPR.*

Alarm Display Design

538 I have minor issues relating to the design of the alarm displays, including the font sizes, which I consider too small to be legible at the expected viewing distance. In addition, consideration should be given to use of uppercase/lowercase fonts in extended textual messages and to the consistent and standard indication of mouse-addressable display points (i.e. targets) on the alarm-related display pages.

539 The demonstrated audible alarm signals appear fit for purpose. However, this will require verification as the design progresses.

> ***AF-UKEPR-HF-43 –*** *The licensee shall justify the design of the audible alarm signals for the UK EPR.*

Alarms and SOA

540 An issue raised by the task analysis of (manual) '*Cross-connection of the Emergency Feedwater Supplies'* is that the operators are prompted to the required local-to-plant action when the EFWS tank level drops to MIN3 level. This is backed by a third priority (yellow) alarm. The action is to ensure water supply to the emergency feedwater tanks. However, this is during SOA response and the operational philosophy during SOA is that the operators are instructed to not respond directly to the alarm system. This contradicts the scenario requirement, which appears to rely on an alarm prompt to ensure a reliable response. This raises a generic issue that there may be other manual actions that rely in part on alarm prompts, although the scenario is a SOA situation and hence the operators, may not be monitoring the alarm system and therefore may miss the alarm prompt.

> ***AF-UKEPR-47 –*** *The licensee shall explain and justify the reliance of any manual actions on response to alarms during SOA operation.*

4.6.5 Procedures

541 These findings relate to item (5) from the methodology and scope presented in Section 3.2.9.

542 I recognise that the detailed design of the procedures is primarily an issue for a prospective licensee organisation. My assessment in GDA Step 4 briefly considers these issues as assumptions are made regarding the quality of procedures in the HRA.

4.6.5.1 State Oriented Approach (SOA)

543 The SOA is common on the existing French NPP fleet, although the implementation proposed for UK EPR is an advanced version supported by a computerised, automatic diagnosis system (AD). AD is a software algorithm which assesses plant status within the context of the SOA. AD thus replicates the manual procedure which is currently applied in the implementation of SOA in French NPPs.

544 SOA is claimed as the principal support to the operator in an incident. It provides guidance on required actions to return the plant to a safe condition. Chapter 18.3 of the November 2009 PCSR (Ref. 17) states:

545 *"The aim of emergency operation is to restore the plant to safe and stable conditions, while ensuring the three fundamental safety objectives are achieved: reactivity control, removal of residual heat, and containment of radioactive material.*

546 *For the UK EPR, the State Oriented Approach (SOA) will be used for developing the emergency operating procedures."*

547 Furthermore, Reference 17 states: "*The State Oriented Approach results in a limited set of strategies designed according to the physical state of the plant, irrespective of the sequence of events or failures that led to this state. The set of emergency operating principles covers all the plant operating conditions."*

548 In the UK EPR, SOA is supported by the AD system which is presented by the PICS. There are three conditions which will cause entry into SOA operation and activation of the AD:

- Activation of a reactor trip or Safety Injection (SI) will automatically trigger AD.
- Occurrence of a fourth (highest) priority level alarm will automatically trigger AD.
- Situations stemming from operating technical specification requirements that require the AD to be activated manually by the operator.

549 In any of these events, the AD alerts the operator via the PICS display and an audible alarm. The AD overview format presented on the PICS is then used. This displays key information regarding plant status (in particular the six critical functions) and the strategy suggested by the AD to address the apparent fault condition including the identification of relevant procedures. Adoption of the SOA follows and operators select the appropriate paper based procedures and gather the required personnel. Remedial actions using the selected procedures are intended to specifically ignore new alarms, making the assumption that the chosen strategy will restore the plant to safe operation.

550 The procedures applied are role specific (OS and OA) and make extensive use of colour coding and flow charts. They also make explicit reference to the PICS display formats required to implement the necessary control actions.

551 Should the PICS be unavailable, then operations using the AD are impossible and operations are transferred to the SICS. EDF and AREVA note this within the PCSR Chapter 7 (Ref. 17) stating: *"In case of unavailability of the PICS due to internal failures, the operating staff decides, on the basis of the messages and alarms from the self-surveillance functions, to transfer operation of the plant from the PICS to the SICS…. When the SICS is put into operation, steady state power operation is continued for a limited time and monitored on the SICS. If the PICS cannot be recovered within 2 to 4 hours, the operators bring the plant to a shutdown state and maintain it in the shutdown state with the SICS"*

552 The written procedures for operating SICS are still under development. Draft specimen FA3 procedures were supplied in response to TQ-UKEPR-1050. They are similar to the printed procedures for PICS operation under SOA direction, and hence the same broad comments apply. However, the drafts were in French and were not reviewed in detail in this assessment.

553 Further description of the intended operation of SOA is provided in Annex 6.

554 Via the PICS interface, I consider that the SOA will provide adequate alerting cues to the operators that a fault condition has occurred. I consider that the layout and presentation of the paper procedures, proposed for use during SOA activity, is clear and makes effective use of colour coding and flow charting. I support the general philosophy of dedicated procedures for the OS and OA roles.

> ***AF-UKEPR-HF-48 –** The licensee shall justify the design of procedures for application on the UK EPR.*

555 I do have a concern that executing the various requirements in the procedures, while taking account of the various "*wait loops*" (i.e. cycling round a discrete element within the procedure) for particular conditions to occur, could result in significant delays. If there are required responses within short time periods, then such delays may be critical. I therefore recommend that validation checks be undertaken using the simulator under realistic conditions, to ensure that key claimed safety actions are appropriately sequenced within the procedures and can be reliably completed within the timescales required by the safety case.

> ***AF-UKEPR-HF-49 –** The licensee shall substantiate that the SOA procedures ensure that claimed safety actions are reliably completed within the timescales required by the safety case.*

556 As conceived, the SOA and its associated materials and interfaces should provide the operators with the required information, particularly regarding the continuous monitoring of the status of critical safety functions. The general supervision of post fault activity by the SS, along with a specific checking function performed by the SE (including using the SICS panel to provide an additional check on critical safety function status), provides error recovery opportunity.

557 Furthermore, the ongoing monitoring provided by the AD function highlights emerging conditions that may affect choices within, or departure from the chosen strategy. This supervisory and monitoring arrangement, and the provision of the SOA overview display should limit poor situational awareness caused by 'cognitive tunnelling'. I recognise that the operators would typically keep the appropriate SOA overview display on one of the five screens available. However, I note that currently there is no requirement on PICS to provide a permanent display of the SOA overview following the onset of AD.

> ***AF-UKEPR-HF-50 –** The licensee shall ensure that the PICS continuously displays an appropriate overview to support implementation of the selected SOA during SOA operation or a justification as to why this is not reasonably practicable.*

558 I note that the OS and OA continually communicated decisions during progress through the strategy, and involved other team members. This communication is likely to assist in the efficient progress through any SOA.

559 There is a lack of information relating to transfer to the SICS panel in general. In particular, despite the noted PICS 'life-sign', I am not clear how a partial failure of PICS, for example in the part of the system responsible for AD, or more insidiously in the information being delivered to the AD, will be noticed by the operators.

> ***AF-UKEPR-HF-51 –** The licensee shall justify the design of the SICS panel and the administrative controls relating to transfer from PICS to SICS.*

4.6.5.2 Normal Operations Computer-Based Procedures

560 During routine operations, all detailed procedures are provided via the PICS with no requirement for paper-based procedures. The OS elects to undertake a strategy for normal operation based on the plant status and considers application of any relevant operating rules. The operating rules specify the operational objectives, their principles and logic together with their justification.

561 Operating Instruction Sheets (MOP) are written based primarily on system design manuals and formalise the step-by-step procedure that the operator must follow. MOPs cover all routine operations and are called upon from the overall operating procedure. Operating Rules may be relevant to the detailed use of some MOP. .

562 MOP are structured computerised procedure formats which are launched by the operator. They do not interact with the process but provide dynamic links to the associated control formats. MOP provide check boxes in which the operator can record completed actions, but these are manually controlled and they only act as a place keeping tool for the operator. The completion of a check box does not relate to actual plant status. There was an intention to allow direct operation of components from the MOP formats, but it was concluded that this was not a desired feature. Operators able to maintain their plant awareness by using the linked status and control formats as advised by the computer-presented instruction.

563 The key elements of the MOP are as follows:

- The header which includes the “MOP Manager”. This is a button bar which allows operator to select and monitor the progress and status of the MOP.
- A text area which provides the purpose and the initial conditions for the MOP.
- A list of the actions in temporal sequence, each has a check box which the operator uses to record completion of each step. The MOP thus describes the actions to take - such as control actions and parameter checks and their correct sequence.
- Dynamic reference hot-points, which when clicked, call up the required status and control formats where the actions are executed.

564 Only the “*active user*” can set the check boxes, any other team member accessing the MOP will see the status of the check boxes but cannot change them. The status of check boxes remains fixed unless altered by the “*active user*”. Any use of a check box is recorded as a unique coded data point so that a history of actions on the MOP can be retrieved if required.

565 The layout of the screen and the check boxes provide a good defence against missing steps in a sequence of actions (further reinforced by the control of only the *“active user”* being able to check a check box) and checks of parameter status. In addition, the fact that the MOP may be accessed by other crew members or may be placed on the POP provides additional team support.

566 The structure of the MOP and the fact that the operator must move to a control format to execute actions will assist situational awareness. The operator also has access to other formats as required, which permits surveillance of other systems while the MOP is being executed, therefore fostering a good understanding of overall plant status.

> ***AF-UKEPR-HF-52 –*** *The licensee shall validate the entire suite of MOP for the UK EPR.*

4.6.6 Staffing and Work Organisation

567 I recognise that the specifics of the staffing levels and work organisation are primarily an issue for a prospective licensee organisation. However, my assessment for GDA Step 4 considers these issues, as assumptions are made in these areas to underpin the HRA and drive the design.

568 My assessment has considered the information regarding staffing the plant during normal and accident situations as described in Chapter 18 of the November 2009 PCSR (Ref. 17). This account is restricted to the proposed crewing of the MCR. The staffing of field operatives and maintenance staff is not addressed. I have assessed the PCSR (Ref. 17) and supplementary information which was provided in Ref. 154 which "..*sets out the principles applied to the organisation of the Flamanville-3 EPR unit…"* and aims to provide "…*the input data needed for establishing operating procedures and for creating the Human-Machine Interface*." and Ref. 69 which describes simulator-based studies aimed at establishing a suitable staffing regime.

569 The November 2009 PCSR (Ref. 17) states: *"The plant is to be run* [from the MCR] *by two operators and a shift supervisor. A similar organisation is used in all French nuclear power stations. This organisation:*

- *Permits a division of work and responsibility to prevent task-overloading of individual operators;*
- *Provides human redundancy in the case of an incident;*
- *Provides coverage for tasks additional to operational management, such as communication, interfacing with maintenance and periodic testing, and*
- *Ensures sufficient personnel are available should multiple [plant] failures occur".*

570 Details on the operating modes and MCR operating team are provided in Annex 5.

571 In brief, the staffing proposed for the MCR is based on the current staffing arrangements in French NPPs; a supervisor and two operators supplemented by a support safety engineer in a fault situation. The duties of the two operators have been modified in the light of OEF and findings from simulator-based HF studies.

572 I have no immediate issues relating to the proposed staffing. However, analysis and evidence will be required to support these manning levels for operation of a UK EPR.

> ***AF-UKEPR-HF-53 –*** *The licensee shall substantiate the proposed manning levels and organisational structure for the UK EPR.*

573 There is evidence (Ref. 69) that EDF and AREVA have considered the distribution of workload between the crew members under the various plant conditions, and that this has resulted in the establishment of the OS and OA roles, which define responsibilities differently to the traditional reactor and secondary side operations. In the scenarios that I observed in the EPR simulator, the two operators co-operated well and undertook the required actions smoothly and effectively. During fault scenarios, the separation of OS and OA roles appeared to result in a fair division of duties such that workload was shared effectively. However, it will be necessary for the workload of MCR personnel to be analysed and justified.

> ***AF-UKEPR-HF-54 –*** *The licensee shall analyse and substantiate the workload levels for UK EPR MCR operators.*

4.6.7 Conclusions

574 My overall judgement is that the quality of the plant-wide human factors across the wide range of areas assessed appears to be adequate and will not significantly undermine human reliability. However, this judgement relies significantly on my inspection of the FA3 simulator due to the lack of detailed evidence provided. Annex 5 gives additional information on my Work Stream 5 assessment.

575 I consider that the MCR design supports the design basis operating organisation (FA3) and use of SOA procedures well.

576 The detailed displays and interfaces for the UK EPR have still to be developed. I have noted several issues (via Assessment Findings) that will need to be addressed both during this detailed design phase and in future V&V of the HMI.

577 To date, there has been virtually no integration between the safety case (including the HRA) and the general HFE design programme. The overall HFE work programme must ensure that the detailed design development work, the PSA/HRA revision and the qualitative human factors substantiation work (in response to the GDA Issue actions) are fully integrated. This should recognise additional claims relating to the SICS panel (and other emerging human based safety claims).

578 Overall there is a considerable volume of work required for a future licensee to develop and justify the detailed UK EPR HMIs.

4.7 Overseas Regulatory Interface

4.7.1 Introduction

579 Our GDA “Strategy for Working with Overseas Regulators” is described in http://www.hse.gov.uk/newreactors/ngn04.pdf. (Ref. 134). This strategy cites the potential benefits of international regulatory collaboration as providing ND with access to independent analyses and audits, the sharing of technical opinions, early advice on construction issues and promotion of a more consistent and harmonised international approach.

580 Additional information is provided in GDA publication “Safety assessment in an International Context” http://www.hse.gov.uk/newreactors/ngn05.pdf (Ref. 135) which explains why the UK has to undertake its own safety assessment for new reactors; how I take into account international standards; and the ways in which I exchange information with overseas regulators on a general basis.

581 For GDA Step 4, HSE committed to reviewing *”overseas progress and issues raised by overseas regulators, yet recognises that the extent to which overseas assessments can be taken into account is dependent on a number of factors including:*

- *The date of the assessment.*
- *The level of detail and the purpose of the assessment.*
- *The local conditions of use relating to the assessment.*
- *The depth of information provided by the Requesting Party including the evidence of issue resolution.*
- *Whether overseas assumptions (e.g. on-plant operating regime) will remain valid if the technology is adopted in the UK.*

- *Whether a demonstration can be made that satisfying the legal requirement that the risks have been reduced to a level that is ALARP.*
- *The scope of HSE's formal information exchange agreements with the overseas regulator.*
- *HSE's knowledge of the overseas regulatory system.*
- *The willingness of the overseas regulator to engage with HSE on issues of primary interest to the UK, including providing access to detailed information."*

582 Our strategy notes that the prime objective of the assessment is to consider the designs against UK requirements. However, where I consider that an overseas regulator's assessment can provide substantial/significant additional assurance, as a result of its scope and rigor, then I will take this into account during my detailed assessment. Furthermore, where another regulator's assessment identifies issues of concern, then I will use this information to help us focus my assessment effort.

583 In light of this published guidance, my strategy in this area was to;

- Establish what information already exists in the areas of HFE and HRA from my international regulator colleagues.
- Determine the relevance of the available information to inform my assessment, considering the issues outlined in the bulleted list above.
- Undertake technical meetings and information exchanges with overseas regulator specialists.

584 The UK EPR design is a joint project being undertaken by EDF and AREVA. It differs to some degree in design details and safety submissions from other EPR projects currently under construction or in the process of design application. This is particularly relevant to aspects of the HF design and safety studies as the UK EPR control room is based on previous French N4 plant and operating approaches, and differs substantially from other AREVA EPR designs. This has limited the benefits that I can take from assessments from overseas regulators.

585 A working group was convened for HF by the Multinational Design Evaluation Programme (MDEP) under the main EPR working group (more information on which can be obtained via http://www.oecd-nea.org/mdep/ (Ref. 136)). However, at the inaugural meeting of the group, it was clear that my assessments were more advanced in both scope and depth than those of my international colleagues. This, coupled with the apparent differences in design and safety submissions between the UK EPR and other EPR designs, meant that I was not able to take any benefit from the working group's assessments and as a result, no further meetings were held.

586 I consulted directly with regulator colleagues in the US NRC, STUK and the Autorité de Sûreté Nucléaire (ASN) the French Authority for Nuclear Safety. A summary of the interactions and how I have taken any assessment benefit from their work is described in Sections 4.7.2, 4.7.3 and 4.7.4.

4.7.2 US Nuclear Regulatory Commission

587 The US NRC operates an entirely different regulatory regime to that of the UK. Its administration is based on prescribed codes and standards to be followed and against which submissions are judged for conformance. This is in contrast to the UK's goal setting (non prescriptive) regime. A further fundamental difference is the concept of

ALARP, which is embodied in UK legislation; its role in the US regulatory system is more limited.

588 The US EPR design and application for certification to the NRC is for an AREVA designed plant. There are design differences between the US and UK EPR designs and the US EPR HRA submissions applies different HRA methods to those for the UK EPR HRA submissions.

589 However, I undertook to understand and judge the relevance of the US assessment of the HFE and the HRA for relevance to my assessment, detail of which are described below:

4.7.2.1 US Nuclear Regulatory Commission Human Factors Engineering

590 The US NRC review of the HFE components of the EPR submission have been delayed several times and at the time of writing was still not available. I note that at an MDEP meeting (non HF) the US NRC cited that the there was *“no major technical issue in this chapter”*. I have not been able to review any US NRC material on the US EPR HFE and hence have taken no benefit from their work.

4.7.2.2 US Nuclear Regulatory Commission Human Reliability Assessment

<u>Introduction</u>

591 I commissioned one of my *TSC* to undertake a review of the applicability of the US NRC assessment of the EPR HRA to the UK. The contractor involved with this work is a former US NRC Senior Level Advisor on PSA / Probabilistic Risk Assessment[6] (PRA) and HRA and a recognised world expert in the field of HRA and PSA / PRA.

592 The review was conducted using publicly available information related to the NRC reviews of the vendor’s submittal for design certification in the USA. The focus was on the NRC reviews of the PSA / PRA used to support the design certification applications, since that is where the technical review of the HRA was conducted. The review was based on: US EPR Safety Evaluation Report With Open Items for the US EPR, Chapter 19, “Probabilistic Risk Assessment and Severe Accident Evaluation” ADAMS Accession # ML090900119.

<u>Background to the US NRC HRA Review</u>

593 The US NRC staff reviews of the PRA were primarily performed to assess whether the PRA model was adequate to identify insights that could be used for the licensing of the plant or for finalising the design.

594 Current US NRC review of a PRA for new reactors is guided by SRP19.0 (Ref. 137) which addresses PRA quality, including HRA, by invoking RG 1.200 (Ref. 138), which in turn endorses the American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS) PRA standard (Ref. 139).

595 SRP Section 19.0 includes the following expectation of how the PRA is to be used in the design stage: *“Identify risk-informed safety insights based on systematic evaluations of the risk associated with the design, construction, and operation of the plant such that the applicant can identify and describe the following:*

[6] Probabilistic Risk Assessment is the equivalent US term for PSA that is more commonly used in Europe.

- *The design's robustness, levels of defense-in-depth, and tolerance of severe accidents initiated by either internal or external events, and*
- *The risk significance of specific human errors associated with the design, and characterize the significant human errors in preparation for better training and more refined procedures."*

596 In the EPR Final Safety Evaluation Report (FSER), the NRC stated: *"the staff finds that the US EPR design-specific PRA is of sufficient quality to be used in the following ways:*

- *to assess the risks associated with the US EPR design*
- *to identify strengths and weaknesses of US EPR design features*
- *to evaluate US EPR containment failure*
- *to compare the risk results with the Commission's safety goal*
- *to provide an integrated perspective of the overall risk estimates for the design*
- *to identify major contributors to the estimated CDF and LRF*
- *to support other programs for certification purposes (e.g., RAP, Maintenance Rule Program (10 CFR 50.65))"*

597 A major element of the HRA is to identify and define the *HFE*s included in the PRA logic model. These were then used to identify the critical or risk-significant human actions. The critical human actions are defined in NUREG-0711 (Ref. 140) to be *"tasks that must be accomplished in order for personnel to perform their functions. In the context of PRA, critical tasks are those that are determined to be significant contributors to plant risk."* From informal discussions with US NRC staff, the HRA quantification method itself was not the most important focus; the primary goal of the review was to assess whether the approach used was acceptable for the purpose of the US NRC review stated above. As discussed later, since the methods used were US NRC-developed methods, their validity was not a concern. The HEPs themselves are recognised as being uncertain, so sensitivity studies are performed to confirm insights.

<u>HRA Methods Used in US Design Certification PRA Submittals</u>

598 The HRA methods applied in the US application for the US EPR were ASEP (NUREG/CR-4772 (Ref. 26)) and SPAR-H (NUREG/CR-6883 (Ref. 27)). Both are US NRC developed methods and there was no US NRC staff concerns with the methods themselves and few questions concerning the performance of the HRA itself.

599 However, at an Advisory Committee on Reactor Safeguards (ACRS) EPR subcommittee meeting on February 19 2010, concern was expressed about the adequacy of SPAR-H as an acceptable HRA method for a PRA during the Combined Operating License (COL) phase, and as a PRA to support risk-informed activities once operation has begun.

<u>Relevance of NRC HRA Reviews to ONR's GDA</u>

600 Based on the documentation reviewed, there appears to be little from the US NRC HRA reviews of the US EPR that can assist my GDA Step 4 assessments of the UK EPR. The usefulness of the US NRC's review of the EPR PRA to my assessment of the UK EPR PSA model is limited by two important factors; the HRA methods applied are different; and the PRA models themselves are different and have modelled different mitigation strategies, resulting in different definitions for *HFE*s and apparently with differing levels of detail.

601 The only area where some benefit could be derived from the PRA is of identification of the critical human actions. While the identification of the *HFEs* in the PRA model is a crucial task of HRA, there is little discussion of how this was reviewed by US NRC.

602 It appears that the US NRC review was undertaken at a much higher level than my Work Stream 2, and performed for an entirely different aim against a prescribed set of criteria not analogous to the goal setting criteria of my HRA TAG.

4.7.3 Säteilyturvakeskus (STUK), Finnish Radiation and Nuclear Safety Authority

603 I undertook discussions in March and November 2010 with HF colleagues in STUK to exchange information on regulatory assessment approaches and assessments of the UK EPR and Olkiluoto 3 (OL3) EPR currently under construction in Finland. The OL3 plant is an AREVA plant design with an AREVA designed main control room that differs to that proposed for the UK EPR.

604 The Finnish process for the granting of a construction license had not included a detailed HF assessment of the design and safety case. STUK are now embarking on a more detailed assessment of HF for OL3. Additionally, the different designs would limit any benefits that can be taken from any work that STUK has undertaken. As a result, I have not been able to take any assessment benefit from the STUK work to date.

4.7.4 Autorité de Sûreté Nucléaire (ASN), French Nuclear Safety Authority

605 The reference plant for the UK EPR is FA3, an EDF and AREVA plant currently under construction in France. ASN have been involved in the assessment of the EPR and the specific FA3 design over several years. Documentation that has been submitted to ASN and a very limited number of letters from ASN, have been submitted as references to the UK EPR PCSR safety submission.

606 ASN’s licensing approach and detailed requirements differ from ONR’s. Notably for HF, there is less emphasis on integration between risk based insights from the PSA and HRA and the HFE programme. ASN has provided an overview of its assessment process for FA3 and from this it is evident that HF is primarily reviewed at the detailed stages of the construction and licensing process. I have been seeking to exchange information on the details of ASN’s assessments of the HF safety case for FA3, but to date very little information has been exchanged, and as a result I have not been able to take any benefit from ASN’s assessments.

5 CONCLUSIONS

607 My GDA Step 4 assessment commenced with consideration of the relevant chapter(s) of the PCSR and supporting references available at that time, and these are referred to as appropriate in this report. As the GDA submission developed during Step 4 in response to my regulatory questions, amendments were made as appropriate to the PCSR and its supporting references. A review has been made of the updates to the GDA submission in my technical topic area and the conclusion of this review is that the updates to, or information included, in the GDA submission and/or supporting references were not as expected and further work is required to address these shortfalls. This will be progressed in GDA through my GDA Issue **GI-UKEPR-HF-01**. For HF, my assessment is therefore limited to the versions of the GDA submission documents referred to in my assessment report. Although the consolidated November 2009 PCSR (Ref. 17) and its supporting references are therefore acceptable as the reference point for an Interim Design Acceptance Confirmation (iDAC), these outstanding issues require acceptable resolution before a final DAC can be issued.

5.1 Overview

608 Overall, I consider that EDF and AREVA have not presented an adequate safety case for HF for the UK EPR and the position has not moved on significantly from the end of GDA Step 3. EDF and AREVA have provided some additional evidence relating to their design process, but much of this was received late in my assessment. They have only been able to provide a very small part of the required substantiation for their key HF claims. This results in a substantial gap in their safety submission for GDA remaining at the end of GDA Step 4.

609 I accept that there is a significant difference in the regulatory approach to HF between the UK and France and I consider that this has contributed to the position. In consequence, I have raised GDA Issue **GI-UKEPR-HF-01** to reflect the significant gap in the safety submission that remains at the end of GDA Step 4.

610 The material that I have assessed to form my judgements has largely been extracted from the considerable amount of documentation provided from the FA3 design. EDF and AREVA have not provided a consolidated HF safety case based on appropriate HF analyses aligned with UK expectations. For the UK EPR, the only targeted HF analysis offered has been the qualitative substantiation of four human based safety claims. This is inadequate for a PCSR. Furthermore, the timing of documentation supplied predominantly in response to regulatory questions and observations, was very late in the GDA Step 4 process and I have not been able to assess it in its entirety.

611 However, I recognise that the UK EPR design is an evolution of a standard PWR and consequently benefits from significant operating experience (particularly relating to N4 and Konvoi plants), and detailed fault studies. I also understand the PSA model and consider that this does not present an exorbitant or sensitive human contribution to the risk and safety of the UK EPR. Furthermore, should subsequent HF assessment reveal further deficiencies in the design or safety analysis, HF solutions can typically be developed and implemented without undue effect on the design of civil structures. On this basis, it is unusual for gross disproportionate arguments to be made relating to HF solutions. I therefore consider that progression post PCSR will not result in the foreclosing of options associated with HF. Consequently, the majority of my conclusions are cited as

Assessment Findings to be taken forward as routine regulatory business post Generic PCSR.

5.2 Assessment Area Conclusions

612 In each of my assessment areas the principal conclusions are:

5.2.1 Work Stream 1 - Substantiation of Human Based Safety Actions

613 Overall I judge that EDF and AREVA have not provided an adequate substantiation of the human based safety claims at the end of GDA Step 4. The main deficiencies are:

- The incompleteness of the identification of human based safety actions, particularly for pre-fault (Type A) activities.
- Inadequate detailed task analysis to support the significant human based safety claims (these are primarily post-fault operator actions). Only four human based safety claims have been analysed.

614 This gap was highlighted in my GDA Step 3 Assessment Report conclusions and identified early on in the GDA Step 4 assessment process.

615 The lack of substantiation I judge to be very significant and has the additional consequence that I consider that EDF and AREVA are not in a position to meet ALARP requirements from a HF perspective. As a result, I propose a GDA Issue (**GI-UKEPR-HF-01** refers) to address both the incompleteness of the identification of human based safety claims and provision of proportionate supporting evidence to support those claims. This also captures my regulatory observations in the areas of pre-fault actions, misdiagnosis, violation and post-fault action substantiation. I have also included a specific action within the GDA Issue for an ALARP justification to be provided.

616 I have collaborated with PSA colleagues and I judge that the HRA and PSA model does provide an acceptable basis for determining the overall risk contribution from human actions at a PCSR stage. I have identified areas of incompleteness and weakness in the HRA, which are cited as Assessment Findings, to be addressed as routine business as the safety case for the UK EPR progresses beyond the design stage. I have aligned these findings with the expectation from my PSA colleagues that the HRA will be updated post the PCSR phase.

617 Additionally, I have noted areas of analytical incompleteness and weakness, which are largely cited as Assessment Findings, to be addressed as routine regulatory business as the safety case for the UK EPR progresses beyond the PCSR stage. I have aligned these findings with the expectation from my PSA colleague that the HRA will be updated post the Generic PCSR phase.

5.2.2 Work Stream 2 - Generic Human Reliability Assessment

618 I judge that the current UK EPR HRA is essentially an ‘assumptions based’ analysis that lacks adequate substantiation from appropriate task analysis of pre and post-fault operator actions. However, my examination of the HRA for both Level 1 and 2 PSA indicates that an acceptable consideration of the contribution from operator error to the overall risk has been made at this point.

619 The HRA method applied to the Level 1 PSA HRA is generally satisfactory, although a greater inclusion of pre-fault human actions (both Type A and B) will be required in the

proposed HRA revision, as will an improved analysis of human error dependency. The consideration of human failure initiating events, particularly for low power and shutdown states, appears to be incomplete and this could be significant. I will take these observations forward as Assessment Findings to be addressed in line with the update of the PSA.

5.2.3 Work Stream 3 - Engineering Systems

620 I consider that EDF and AREVA have undertaken work related to maintenance, which has the potential to support human reliability and there is some evidence of the application of operational experience and design input to support their claims in this area. However, there appears to have been strong reliance on design guidance supplied to designers and contractors. In recognition of the uncertainty I have over the adequacy of EDF and AREVA's approach, I propose to take my assessment observations forward in two ways; via GDA Issue Action **GI-UKEPR-HF-01.A1** relating to the consideration of pre-fault human actions; and via Assessment Findings relating to the detailed design and verification requirements for the UK EPR equipment.

5.2.4 Work Stream 4 - HF Integration

621 In general, I judge that EDF and AREVA have evidence of aspects of a HFE programme of work but not of an overall HFI plan that meets my expectations. What has been provided is 'piecemeal' and is focused on the MCR design. There has been an over-reliance on the use of operational experience, rather than formal safety analysis and on design guidance provided to engineers. This does not provide me with confidence that the risk from human error has been reduced to ALARP. However, as HFI is process based, this will be taken forward via an Assessment Finding to be addressed by a prospective licensee.

5.2.5 Work Stream 5 – Plant-wide Generic HF Assessment

622 I consider that in general the quality of the design based HF aspects across the wide range of areas assessed (AoF; Workplace and workstation design; Working environment; Control and Display interfaces; Procedures; and Staffing and work organisation) appear to be adequate and will not significantly undermine human reliability.

623 I judge that the MCR design supports the design basis operating organisation (FA3) and use of SOA procedures well. However, I note many minor observations across the assessment area and these are cited as Assessment Findings to be addressed post PCSR. However, due to the limited evidence provided in GDA Step 4, there will be a significant requirement for a future licensee to undertake detailed studies to confirm the adequacy of the design, particularly for non-MCR locations. Again, I have cited these specific requirements as Assessment Findings.

624 Table 13 collates the 'results' that have emerged from each assessment work stream in terms of Assessment Findings and GDA Issues. The Assessment Findings noted for each work stream are all those which relate to the Work Stream. This therefore does include some duplication where Assessment Findings relate to more than one work stream.

Table 13: Assessment Findings and GDA Issues per Work Stream

Assessment Work Stream	Number of Assessment Findings	Number of GDA Issues
1	6	1
2	15	0
3	2	0
4	8	0
5	24	0

5.3 Meaningful Generic Design Assessment

625 I judge that the assessment that I have undertaken of the human contribution to safety for the UK EPR is a meaningful GDA. Ref. 173 notes that *"A meaningful GDA will be one where : the regulators have received sufficient information on the generic reactor design in the safety…..submissions to allow assessment in all relevant technical topic areas; and the regulators have completed a sufficiently thorough and detailed assessment of the information in the generic safety….submissions".*

626 I consider that I have received sufficient information and have undertaken a sufficiently thorough and detailed assessment of that information.

627 Ref. 173 recognises that this *"does not mean that the regulators have received and assessed all the information necessary to permit construction and operation of a plant, based on that design, at a specific site in the UK"*. This is the case for HF and is reflected via my GDA Issue and Assessment Findings.

5.4 Global Judgements on Adequacy

628 TAG T/AST/051 (Ref. 7) provides overarching expectations on the 'Purpose, Scope and Content of Nuclear Safety Cases'. In this section I offer commentary on the EDF and AREVA position for HF against those broad expectations.

629 *Completeness:* TAG T/AST/051 requires that *"all reasonably foreseeable threats to safety should be identified. It should be shown that the plant incorporates adequate protection against these threats, or that their contribution to the overall risk is negligible."* I consider that the EDF and AREVA case is 'incomplete' in terms of justification of operator claims that support the overall UK EPR safety case. However, I judge that the 'claims' represented in the HRA and PSA are sufficiently complete to judge their overall risk contribution at the Generic PCSR stage. I consider that there is a considerable amount of work required to substantiate the key claims for human based safety actions and additional work to complete the full identification of claims to complete the case.

630 *Clear:* the expectation is that *"….there should be a clear statement as to the nature and magnitude of the significant hazards, and the protection in place to prevent or mitigate the effects. The safety case needs to be readily accessible as well as understandable. It should be possible to navigate easily around…to find the relevant information"*. I consider that EDF and AREVA have not presented a clear consolidated safety case for HF at GDA Step 4. I have struggled to find the relevant material from the submissions provided. I have addressed this in action A2 of GDA Issue **GI-UKEPR-HF-01**.

631 Further requirements are that "*the basis of all assumptions, conclusions and recommendations should be given*". I do not consider that the basis of all assumptions is provided; and this is noted in my Work Stream 1 assessment.

632 *Rational: "the safety case should be reasonable and sensible. It should provide cogent, cohesive and logical arguments to support the conclusions"*. I consider that EDF and AREVA have not presented their HF safety case in a logical manner, particularly in line with the claims/arguments/evidence format. There has been a marked improvement in the recent submissions and EDF and AREVA have indicated their intent to provide an updated HF safety case that meets my expectations in terms of clarity and format.

633 *Accurate:* The safety case should accurately reflect the 'as is' state of the plant, equipment, processes and procedures. I consider that the HF safety case is accurate to a point, recognising the development stage of the design however, I note that the HRA does not reflect the 'as is' state of the 'plant, equipment, processes and procedures, largely due to the lack of underpinning task analysis. This has been discussed widely in my assessment.

634 *Appropriate:* This essentially relates to the appropriateness of the methods used to substantiate safety. I have discussed this in my assessment and am generally content with the HRA methods used. The sample provided of task analyses for some key claims are of high quality and I expect that the future work to address the GDA Issue will be of similar standard.

635 *Integrated: "the safety case should be holistic so that there are clear links between the safety analysis and engineering substantiation"*. This is a main area of non conformance in my opinion as the qualitative HF analysis is not linked back directly to the underpinning of the quantitative HRA. I also consider that the HF safety case largely stands alone and is not integrated into related technical discipline assessment to provide a holistic safety case / PCSR.

636 Current: This relates to the requirement to review, revise and update the safety case to maintain its currency. This is not applicable to GDA.

637 Forward Looking: The safety case should demonstrate that the plant will remain safe throughout a defined life time. I have noted that there are limitations in the information provided on the HF contribution to the decommissioning plan and I have cited an Assessment Finding in this regard.

638 To conclude, I judge that EDF and AREVA have not provided an adequate substantiation of the human based safety claims at the end of GDA Step 4. The main deficiencies are incompleteness of identification and the lack of substantiation of human based safety claims. However, I do not object to progression of the UK EPR design on HF grounds principally due to the fact that it is an evolution of a standard PWR, which benefits from significant operating experience (particularly relating to N4 and Konvoi plants) and detailed fault studies. I also understand the PSA model and consider that this does not present an exorbitant or sensitive human contribution to the risk and safety of the UK EPR. Furthermore, should subsequent HF assessments reveal further deficiencies in the design or safety analysis, HF solutions can typically be developed and implemented without undue effect on the design of civil structures. On this basis, it is unusual for gross disproportionate arguments to be made relating to HF solutions. I therefore consider that progression, post PCSR, will not result in the foreclosing of options associated with HF

639 However, this conclusion is subject to satisfactory progression and resolution of the GDA Issue to be addressed during the forward programme for this reactor and assessment of

additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.4.1 Assessment Findings

640 I conclude that the Assessment Findings listed in Annex 1 should be implemented through a forward programme for this reactor as routine regulatory business.

5.4.2 Generic Design Assessment Issues

641 I conclude that the GDA Issue listed in Annex 2 must be satisfactorily addressed before Consent will be granted for the commencement of nuclear island safety-related construction.

6 REFERENCES

1 *GDA Step 4 Human Factors Assessment Plan for the EDF and AREVA UK EPR.* HSE-ND Assessment Plan AR 09/064. April 2010. TRIM Ref. 2009/471068.

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

3 *ND BMS. Technical Reports.* AST/003 Issue 3. HSE. November 2009. www.hse.gov.uk/foi/internalops/nsd/assessment/ast003.htm

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

5 *Nuclear power station generic design assessment – guidance to requesting parties.* Version 3. HSE. August 2008. http://www.hse.gov.uk/newreactors/guidance.htm.

6 *Step 3 Human Factors Assessment of the EDF and AREVA UK EPR*. HSE-ND Assessment Report AR 09/031. November 2009. TRIM Ref. 2009/335835.

7 *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/tast10.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

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

9 *Standard Review Plan.* NUREG-0800 Draft Revision 3. US Nuclear Regulatory Commission. June 1996.

10 *Human-System Interface Design Review Guideline.* NUREG-0700 Revision 2. US Nuclear Regulatory Commission. May 2002.

11 *Title 10, Code of Federal Regulations, Part 50, Domestic licensing of production and utilization facilities*. US Nuclear Regulatory Commission Regulations.

12 *Title 10, Code of Federal Regulations, Part 52*, *Licenses, certifications, and approvals for nuclear power plants*. US Nuclear Regulatory Commission Regulations.

13 *Swain A D and Guttman H E. Handbook of human reliability analysis with emphasis on nuclear power plant applications.* NUREG/CR-1278. 1983.

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

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

16 *EDF and AREVA UK EPR - Schedule of Regulatory Issues Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600728.

17 *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.

18 *UK EPR Master Submission List.* November 2009. TRIM Ref. 2011/46364.

19 *Step 3 Radiological Protection Assessment of the EDF and AREVA UK EPR. HSE-ND Assessment Report AR 09/030. November 2009. TRIM Ref. 2009/335834.*

20 Not used.

21 Not used.

22 *Sheue-Ling Hwang, Guo-Feng Liang, Jhih-Tsong Lin, Yi-Jan Yau, Tzu-Chung Yenn, Chong-Cheng Hsu, Chang-Fu Chuang. A real-time warning model for teamwork performance and system safety in nuclear power plants*. Safety Science. pp 425–435. Volume 47. March 2009.

23 *Workman M. The effects of technology- mediated interaction and openness in virtual team performance measures.* Behaviour and Information Technology. pp 355-365. Volume 26. September 2007.

24 *Parush A. An empirical evaluation of textual display configurations for supervisory tasks.* Behaviour and Information Technology. pp 225-235. Volume 23. July 2004.

25 *Javaux D. A method for predicting errors when interacting with finite state systems. How implicit learning shapes the user's knowledge of a system.* Reliability Engineering and System Safety. pp 147-165. February 2002.

26 *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. NUREG/CR–4772. Sandia National Laboratories. February 1987.

27 *The SPAR-H Human Reliability Analysis Method*. NUREG/CR–6883. Idaho National Laboratory. August 2005.

28 *Identification and Substantiation of Key Claims on Operator Reliability in the UK EPR PSA Level 1*. NEPS-F/10.173. AREVA. February 2010. TRIM Ref. 2011/155355.

29 *Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment*. NEPS-F DC 191 Revision A. AREVA. January 2010. TRIM Ref. 2011/92797.

30 *UK EPR Level 2 Supporting Human Reliability Analysis*. NEPS-F DC 527 Revision A. AREVA. December 2010. TRIM Ref. 2011/92809.

31 Not used.

32 *Cepin M. DEPEND-HRA – A method for consideration of dependency in human reliability analysis*. Reliability Engineering and System Safety. pp 1452-1460. Volume 93. Issue 10. October 2008.

33 Not used.

34 *UK EPR Probabilistic Safety Analysis Level 1 Detailed Documentation.* NEPS-F DC 355 Revision B. AREVA. August 2008. TRIM Ref. 2011/85677.

35 *Hannaman G W, Spurgin A J and Lukic Y D. Human Cognitive Reliability Model for PRA Analysis.* NUS-4531. NUS Corporation, prepared for the Electric Power Research Institute, Palo Alto, Ca. 1984. Also summarized in “A Model for Assessing Human Cognitive Reliability in PRA Studies”, Hannaman G W et al. IEEE Third Conference on Human Factors and Nuclear Safety. Institute of Electrical and Electronics Engineers. New York. 1985.

36 *Operator Reliability Experiments Using Power Plant Simulators: Volume 2: Technical Report.* EPRI NP-6937. Electric Power Research Institute (EPRI). July 1990.

37 *An Overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards.* ECEF100427 Revision A. EDF. March 2010. TRIM Ref. 2011/92105.

38 *RO-UKEPR-79A.1 – Human Factors Assessment of Misdiagnosis Potential.* Letter from UK EPR Project Front Office to ND. EPR00737R. December 2010. TRIM Ref. 2011/139.

39 *RO-UKEPR-80A.1-UKEPR - Human Factors Assessment of Violations Potential***.** Letter from UK EPR Project Front Office to ND. EPR00744R. January 2011. TRIM Ref. 2011/29422.

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

41 *EDF/AREVA GDA Task Analysis for Example Claim 1: Start-up of the Station Blackout Diesel Generators following a Loss of Offsite Power*. 16474/TR/002 Issue 02. AMEC. July 2010. TRIM Ref. 2011/92915.

42 *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.

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

44 *Response to Level 3 Human Factors Topic Meeting Action 5-HF-3: Forward Programme of Human Factors Analysis to address Regulatory Observation Action RO-UKEPR-38-A1.* Letter from UK EPR Project Front Office to ND. EPR00374N. April 2010. TRIM Ref. 2010/196510.

45 *Summary and results of the FA3 and 4 ETB ergonomic study.* ECEP060987 Revision A1. EDF. February 2007. TRIM Ref. 2011/137634.

46 *EPR - Optimisation of radiological protection activities – “Reactor pressure vessel opening/closing” Section 1*. ECEMA050275 Revision C1. EDF. February 2009. TRIM Ref. 2011/137626.

47 *EPR - Optimisation of activities with of significant radiological protection hazard – ‘Fuel Removal’ – Stage 1.* ECEMA050056 Revision A1. EDF. March 2009. TRIM Ref. 2011/85559.

48 *EPR Optimisation of activities with a radiation protection requirement involved in waste processing: Sections 1 and 2*. D4002.92.06/123 Revision 1EN. EDF. May 2010. TRIM Ref. 2011/93916.

49 *Operating Feedback Study on the N4 plant series for EPR – Local activity at Chooz. NPP* EDF. 2002.

50 *Example of a fuel handling analysis: Taking account of Human Factors for fuel handling activities*. ECEP071048 Revision A. EDF. July 2007. TRIM Ref. 2011/137605.

51 *Moreau S. PCSR – Sub-chapter 12.4 – Dose uptake optimisation*. UKEPR-0002-124 Issue 02. Areva NP and EDF. 17 June 2009.

52 *Reactor Building Specifications*. ECIG0001089 Revision C1. EDF. September 2009. TRIM Ref. 2011/137568.

53 *EPR – Technical Specifications for the Diesel Buildings*. ECEIG0000756 Revision C. EDF. September 2007. TRIM Ref. 2011/137547.

54 *Book of Technical Specifications; Valves for Nuclear Power Plants*. CST 45.C.015 EN Revision 00. EDF. March 2009. TRIM Ref. 2011/93840.

55 *Procedure MIP EPR No 2.64 Installation Guide – Consideration of Human Factors*. ECEIG0100625 Revision A. EDF. December 2001. TRIM Ref. 2011/137540.

56 *Process for Monitoring of Installation Studies and Tracking of PDMS model data modifications, by Building*. ECEIG070082 Revision A. EDF. June 2007. TRIM Ref. 2011/137530.

57 *Monitoring Programme for Sofinel Civil contract*. ECEIG050365 Revision A. EDF. May 2006. TRIM Ref. 2011/92108.

58 *Monitoring Programme for Areva Civil contract*. ECEIG050444 Revision A. EDF. November 2005. TRIM Ref. 2011/137503.

59 *EPR – Optimisation of Activities with radiation protection risk “RCP, RCV, RIS/RRA, [RCS, CVCS, SIS/RHRS] Valves” – Section 1.* ECEMA050230 Revision B1. EDF. October 2007. TRIM Ref. 2011/155854.

60 *Technical specifications and conditions: Functional expression of Need*. CCF 04 Revision E. EDF. October 2009. TRIM Ref. 2011/86868.

61 *Human Factors programme for evaluation of the EPR’s operating means before the 1st fuel loading*. H-T54-2007-01446-FR Version 1.0. EDF. January 2008. TRIM Ref. 2011/94074. .

62 *Approach for Integration of Human Factors in EPR Design*. ECEF012001 Revision A. EDF. December 2001. TRIM Ref. 2011/155700.

63 *UK EPR – HF Organogram – Topic Meeting Action 1-HF-02*. Letter from UK EPR Project Front Office to ND. EPR00169N. 2 September 2009. TRIM Ref. 2009/358364.

64 *Sheet C5 Control Rooms and Annexes*. ECEIG0100002/SRE Revision A1. EDF. March 2010. TRIM Ref. 2011/92106.

65 *Summary and Results of the FA3 and 4 ETB Ergonomic Study*. ECEP060987 Revision A1. EDF. February 2007. TRIM Ref. 2011/155865.

66 *EPR computerised operation: protocol for complementary tests*. HT– 54/05/021/A Revision A. EDF. January 2006. TRIM Ref. 2011/94147.

67 *Feasibility Study on Application of DPN Specifications to EPR Computerised Operation*. ECEF032026 Revision A1. EDF. 2003. TRIM Ref. 2011/92104.

68 *EPR Computerised Operation: Protocol for Evaluation Tests Relative Operation Department requirements*. HT54/03/016 Revision A. EDF. December 2003. TRIM Ref. 2011/94110.

69 *EPR HMI – Evaluation of the principles of computerised operation – assessment of the 2005 supplementary test campaign.* ECEF060191 Revision A1. EDF. 2005. TRIM Ref. 2011/155719.

70 Not used.

71 *Procedure For Taking Into Account Human Factors In Fuel Handling Operations*. ECEP071048 Revision A. EDF. July 2007. TRIM Ref. 2011/155867.

72 Contract YR2601 - *Fuel Handling System Technical Specifications – Section 1 General Requirements PMC-PTR-PMO DMK.* SFL-EFMF 006.109 Revision F. Sofinel. 29 October 2010. TRIM Ref. 2011/155447.

73 *RO-UKEPR-79A.1 - Human Factors Assessment of Misdiagnosis Potential*. Letter from UK EPR Project Front Office to ND. EPR00737R. December 2010. TRIM Ref. 2011/139.

74 *RO-UKEPR-80A.1 – UKEPR - Human Factors Assessment of Violations Potential*. Letter from UK EPR Project Front Office to ND. EPR00744R. January 2011. TRIM Ref. 2011/29422.

75 *N4 and EPR computerised operation principles*. UKEPR-0014-001 Issue 00. EDF. December 2009. TRIM Ref. 2011/94407.

76 *Interface Protocol between HSE Nuclear Directorate / Environment Agency and Requesting Parties*. JPO/003 Issue 2. HSE. August 2008. TRIM Ref. 2008/41861.

77 *HFI Management Guide (formerly STGP10).* MAP-01-010 Issue 4. MOD Sea Systems Group. November 2006.

78 *The MOD HFI Process Handbook*. Edition 1. UK Ministry of Defence. August 2007.

79 *Human Factors Engineering Program Review Model.* NUREG-0711 Revision 2. US Nuclear Regulatory Commission (USNRC). February 2004.

80 *ISO 9241-210:2010. Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems*. International Organisation for Standardization (ISO). 2010.

81 *ISO/TR 18529: 2000. Ergonomics of Human-System Interaction – Human-Centred Lifecycle Process Descriptions*. International Organisation for Standardization (ISO). 2000.

82 *Human Factors for Designers of Systems. Part 0: Human Factors Integration*. *DEFSTAN 00-250 Part 0.* Ministry of Defence. Issue 1. 23 May 2008.

83 *ISO 11064-7:2006. Ergonomic Design of Control Centres – Part 7: Principles for the design of control centres.* International Standards Organisation. Geneva. 2006.

84 *Kroemer K H E and Grandjean E. Fitting the Task to the Human.* 2001. ISBN 0-7484-0665-4.

85 *Pheasant S and Haslegrave C M. Bodyspace – Anthropometry, Ergonomics and the Design of Work.* 2006. ISBN 0-7484-0067-2

86 *Mechan J. Extending DISC Interface Design for Ergonomists (IDER) and Design of Interfaces for Station Control Rooms (DISC).* HF/GNSR/5043. University of Nottingham. 1998.

87 Not used.

88 *Identification and Substantiation of Key Claims on Operator Reliability in the UKEPR PSA Level 2*. NEPS-F/10.273. Areva. March 2010. TRIM Ref. 2011/155356.

89 *Response Plan RO-UKEPR-38 – The Role of Human Actions on the UK EPR and associated Regulatory Observation Action RO-UKEPR-38-A1.* Letter from UK EPR Project front Office to ND. EPR00237N. December 2009. TRIM Ref. 2009/506375.

90 *Lind M, Seipel S and Mattiason C. Displaying meta-information in context*. Behaviour and Information Technology, Volume 20 Issue 6, pp427-432. January 2001.

91 *Müsseler J, Meiunecke C, Döbler J. Complexity of user interfaces: Can it be reduced by a mode key?* Behaviour and Information Technology. Volume 15 Issue 5. pp 291-300. January 1996.

92 *Wiedenbeck, S. The use of icons and labels in an end-user application program: an empirical study of learning and retention*. Behaviour and Information Technology, Volume 18 Issue 2. pp 68-82. January 1999.

93 *Bétrancourt, M. and Bisseret, A. Integrating textual and pictorial information via pop-up windows: an experimental study*. Behaviour and Information Technology. Volume 17 Issue 5. pp 263-273. January 1998.

94 *Carey J M, Mizzi PJ and Lindstrom LC. Pull-down versus traditional menu types: an empirical comparison*. Behaviour and Information Technology. Volume 15 Issue 2. pp 84-95. January 1996.

95 *Fischer, S. and Doherty, U. Adaptively shortened pull-down menus: location knowledge and selection efficiency*. Behaviour and Information Technology. Volume 27 Issue 5. pp 439-444. September 2008.

96 *Snowberry K, Parkinson S, and Sisson N. Effects of help fields on navigating through hierarchical menu structures*. International Journal of Man-Machine Studies. Volume 22 Issue 4. pp 479-491. Cited in O'Hara et al. 1985.

97 *Kunkel K, Bannert M, and Fach P W. The influence of design decisions on the usability of direct manipulation user interfaces*. Behaviour and Information Technology. Volume 14 Issue 2. pp 93-106. 1995.

98 *Jorgensen A H, Garde A H, Laursen B and Jensen B R. Using mouse and keyboard under time pressure: preference, strategies and learning*. Behaviour and Information Technology. Volume 21 Issue 5. pp 317-319. January 2002.

99 *Trewin S and Pain H. A model of keyboard configuration requirements*. Behaviour and Information Technology. Volume 18 Issue 1. pp 27-35. January 1999.

100 *Scott Mackenzie I and Zhang S X. An empirical investigation of the novice experience with soft keyboards*. Behaviour and Information Technology. Volume 20 Issue 6. pp 411-418. January 2001.

101 *Nordby K, Raanas R K and Magnussen S. The expanding telephone number Part 1: Keying briefly presented multiple-digit numbers*. Behaviour and Information Technology. Volume 21 Issue 1. pp 27-38. January 2002.

102 Shryane N M , Westerman S J, Crawshaw C M, Hockey G R J and Sauer J. Task analysis for the investigation of human error in safety critical software design: a convergent methods approach. Ergonomics. Volume 41 Issue 11. pp 1719-1736. November 1998.

103 *Ockerman J J and Pritchett A R. Improving performance on procedural tasks through presentation of locational procedure context: an empirical evaluation*. Behaviour and Information Technology. Volume 23 Issue1. pp11-20. January 2004.

104 *Lin D-Y M, Su Y-L. The effect of time pressure on expert system based training for emergency management*. Behaviour and Information Technology. Volume 17 Issue 4. pp195-202. January 1998.

105 *Kontogiannis T. and Moustakis V. An experimental evaluation of comprehensibility aspects of knowledge structures derived through induction technique: a case study of industrial false diagnosis*. Behaviour and Information Technology. Volume 21 Issue 2. pp117-135. January 2002.

106 *Ozok A A and Salvendy G. The effect of language inconsistency on performance and satisfaction in using the Web: results from three experiments*. Behaviour and Information Technology. Volume 22 Issue 3. pp155-163. May 2003.

107 *Tractinsky N. A theoretical framework and empirical examination of the effects of foreign and translated Interface language*. Behaviour and Information Technology. Volume 19 Issue 1. pp 1-13. January 2000.

108 *Renaud K, and Ramsay J. Now what was that password again? A more flexible way of identifying and authenticating our seniors*. Behaviour and Information Technology. Volume 26 Issue 4. pp 309-322. July 2007.

109 *Molich R and Dumas J S. Comparative Usability Evaluation (CUE-4).* Behaviour and Information Technology. Volume 27 Issue 3. pp 263-281. May 2008.

110 *Broberg H, Massaiua S, Julius J and Johansson B. The International HRA Empirical Study: Simulator results from the loss of feedwater scenarios*. Proceedings of PSAM 10. June 2010.

111 *Beare A N, Dorris R E, Bovell C R, Crowe D S and Kozinsky E J. Simulator-based study of human errors in nuclear power plant control room tasks*. NUREG/CR-3309. US Nuclear Regulatory Commission. 1984.

112 *Dougherty E M and Collins E P. Assessing the Reliability of Skilled Performance*. Journal of Reliability Engineering and System Safety. Volume 51 Issue 1. pp35-42. January 1996.

113 *Williams J C. A User Manual for the HEART Human Reliability Assessment Method*. DNV Technica Report C2547. (unpublished). 1992.

114 *The International HRA Empirical Study - Phase 2 Report - Results From Comparing HRA Methods Predictions To Hammlab Simulator Data On SGTR Scenarios.* HWR-915 Appendix A. OECD Halden Reactor Project. March 2010.

115 Not used.

116 *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. Specific Safety Guide No SSG-3. International Atomic Energy Agency (IAEA). 2010.

117 *Chang, Y. H. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents (ADS-IDACrew*). 1999.

118 *Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants*. IAEA-TECDOC-1151. International Atomic Energy Agency. July 2006.

119 *Good Practices for Implementing Human Reliability Analysis (HRA).* NUREG-1792. U.S. Nuclear Regulatory Commission. 2004.

120 *Evaluation of Human Reliability Analysis Methods Against Good Practices*. NUREG-1842. U.S. Nuclear Regulatory Commission. 2006.

121 *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*. TR-100259. Electric Power Research Institute (EPRI). 1992.

122 *Julius J, Grobbelaar J, Spiegel D and Rahn F. The EPRI HRA Calculator® User's Manual Version 3.0*. Product ID 1008238. Electric Power Research Institute (EPRI), May 2005.

123 *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*. NUREG/CR-3518, Volumes I and II. U.S. Nuclear Regulatory Commission. 1984.

124 *Chien S H, Dykes A A, Stetkar J W and Bley D C. Quantification of Human Error Rates Using a SLIM-Based Approach*. Conference Record for IEEE Fourth Conference on Human Factors and Power Plants. 1988.

125 *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624 Revision 1. U.S. Nuclear Regulatory Commission. 2000.

126 *Systematic Human Action Reliability Procedure (SHARP).* EPRI-NP-3583. Electric Power Research Institute (EPRI). 1984.

127 *Chandler F T et al. Human Reliability Analysis Methods Guidance for NASA*. NASA/OSMA Technical Report. 2006.

128 *Hollnagel E. Cognitive Reliability and Error Analysis Method (CREAM).* Elsevier. 1998. ISBN: 0-08-042848-7.

129 *Kirwan B, Gibson H, Kennedy R, Edmunds J, Cooksley G and Umbers I. Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool*. 7th Probabilistic Safety Assessment and Management (PSAM) Conference. 2004.

130 *Sträeter O. Cognition and safety - An Integrated Approach to Systems Design and Performance Assessment*. 2005. ISBN:978-0754643258.

131 *Shen S H and Mosleh A. Human Error Probability Methodology Report*. RAN: 96-002: Calvert Cliffs Nuclear Power Plant: BGE. 1996.

132 *Reer B, Dang V N and Hirschberg S. The CESA Method and its Application in a Plant-Specific Pilot Study on Errors of Commission*. Reliability Engineering and System Safety. Volume 83 Issue 2 pp 187-205. February 2004.

133 *Broughton J et al. Human Factors Process Failure Modes and Effects Analysis*. PGOC91-F050-JMS-99286: Boeing. 1999 .

134 *New Nuclear Power Stations. Generic Design Assessment. Strategy for Working with Overseas Regulators.* NGN04. HSE. April 2009. www.hse.gov.uk/newreactors/ngn04.pdf

135 *New Nuclear Power Stations. Generic Design Assessment. Safety assessment in an International Context*. NGN05 Version 3. HSE. March 2009. www.hse.gov.uk/newreactors/ngn05.pdf

136 OECD MDEP Website. www.oecd-nea.org/mdep/.

137 *Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors. Review Plan Section 19.0*. NUREG-0800 Standard Revision 2. USNRC. June 2007.

138 *An Approach for Determining the technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*. Regulatory Guide 1.200 Revision 2. USNRC. March 2009.

139 *Standard for Level1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications: Addenda to ASME/ANS RA-S-2008*. ASME/ANS RA-Sa-2009. American Society of Mechanical Engineers (ASME). 2009.

140 *Human Factors Engineering – Program Review Model*. NUREG-0711 Revision 1. USNRC. February 2004.

141 *ENG 2.21 Procedure: Degree of Automation for Plant Systems*. ECEF02 1855 Revision B1. EDF. May 2006. TRIM Ref. 2011/155703.

142 *Technical Specifications and Conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scope simulator room of the EPR France Plant*. ECECC041294 Revision C1. EDF. 2005. TRIM Ref. 2011/92103.

143 *Health Survey for England – 2008: Trend Tables*. NHS. 2008.

144 *Sheet C5 – Control Rooms and Annexes*. ECEIG0100002 Revision A1. EDF. 2001. TRIM Ref. 2011/92106.

145 *Kroemer K.H.E, and Grandjean E. Fitting the Task to the Human: A Textbook of Occupational Ergonomics*. 1997. ISBN: 978-0748406654.

146 *Human-System Interface Design Review Guidelines*. NUREG-0700 Revision 2. US NRC. May 2002.

147 *EPR Operations Display Engineering Rule EG 02-34"Display Specification".* ECEF040974 Revision B1. EDF. June 2006. TRIM Ref. 2011/155708.

148 *Report on recorded differences between Operator Workstation Panel HMI on Plant Unit and Operator Workstation HMI on Phase 2 Simulator*. ECECC090517 Revision B1. EDF. 2010. TRIM Ref. 2011/85886.

149 *Sizing of SICS.* ECEF021069 Revision C1. EDF. March 2008. TRIM Ref. 2011/86541.

150 *SICS Operating principles.* ENFCR1090069 A. EDF. March 2009. TRIM Ref. 2011/93975.

151 *ENG 2-33 Procedure: Principles for specifying and handling alarms for EPRENG 2-33 Procedure: Principles for specifying and handling alarms for EPR.* ECEF040683 Revision C1. EDF. August 2008. TRIM Ref. 2011/85891.

152 Not used.

153 Not used.

154 *Guiding Principles Relating to the Organization of the Flamanville 3 Shift Crew* D4002.92-07/084. EDF. February 2010.

155 *GDA Issue GI-UKEPR-HF-01 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81192.

156 *Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-022 Revision 0. TRIM Ref. 2010/581510.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
Work Stream 1	
NEPS-F DC 191, Rev A. January 2010. AREVA.	Human Reliability Analysis Notebook of the UKEPR Probabilistic Safety Analysis.
NEPS-F/10.173. February 2010. AREVA.	Identification and Substantiation of Key Claims on Operator Reliability in the UKEPR PSA Level 1.
NEPS-F/10.273. March 2010. AREVA.	Identification and Substantiation of Key Claims on Operator Reliability in the UKEPR PSA Level 2.
UKEPR0002 Issue 4 November 2009.	UK EPR PCSR.
ECEF 100427_CCI, Rev A. March 2010. EDF.	An Overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards.
NEPS-F DC-355 Rev B FIN 2008. AREVA.	UKEPR Probabilistic Safety Analysis Level 1 Detailed Documentation.
16474/TR/002. Issue 02 July 2010. AMEC.	EDF and AREVA GDA Task Analysis for Example Claim 1: Start-up of Station Blackout Diesels following a Loss of Offsite Power.
16474/TR/0003. Issue 02 September 2010. AMEC.	EDF and AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims.
16474/TR/005. Issue 02 November 2010. AMEC.	EDF and AREVA GDA Task Analysis: Example Pre Fault Analysis.
16474/TR/006. Issue 01 December 2010. AMEC.	EDF and AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK].
ND EPR00374N.	Letter on Forward Programme of HF Analysis.
UKEPR-0005-001. Issue 00 dated June 2008.	Comparison of EPR design with HSE/NII SAPs.
16474/TR/001. Issue 01 July 2010. AMEC.	EDF/AREVA GDA Task Analysis Method Statement.
Annex 1 to Letter ND EPR00591N.	EDF/AREVA GDA Task Analysis Method Statement Claim 2: Pre-Fault Human Errors.
Annex 2 to Letter ND EPR00591N.	EDF/AREVA GDA Task Analysis Method Statement Claim 3: Human Errors Performed on Systems and Equipment not modelled in the PSA.
ND EPR00737R 31 December 2010.	Human Factors Assessment of Misdiagnosis Potential.
ND EPR00744R 12 January 2011.	Human Factors Assessment of Violations Potential.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
Work Stream 2	
UKEPR-0002-15, 1 Issue 02 (2009).	PCSR – Sub-chapter 15.1 – Level 1 PSA. EDF and AREVA.
	TQ-EPR-297 (2009) Sequence Timing. AREVA.
NEPS-F/10.173. February 2010. AREVA.	Identification and Substantiation of Key Claims on Operator Reliability in the UK EPR PSA Level 1.
NEPS-F DC 191, Rev A. January 2010. AREVA.	Human Reliability Analysis Notebook of The UK EPR Probabilistic Safety Analysis.
NEPS-F DC 527, Rev A. December 2010. AREVA.	UK EPR Level 2 Supporting Human Reliability Analysis.
Work Stream 3	
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 1.2 – General description of the unit.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 18.1 – Human-Machine Interface.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 18.2 – Normal Operation.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 3 – General Design and Safety aspects.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 7 – Instrument and Control.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 12 – Radiation protection measures.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 15 – Probabilistic Risk Analysis.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 17 – Compliance with ALARP principles.
UKEPR-0002-012. Issue 01 (2009).	PCSR – Sub-chapter 21 – Quality and project management.
ECEPEP 040070. April 2004. EDF.	Letter and annex 'Analysis of Local Maintenance and Operating Activities Selection and Disciplines involved'.
ECEF012001, Rev A. December 2001. EDF.	Approach for Integration of Human Factors in EPR design.
UKEPR-0005-001. Issue 00 (2008).	Comparison of EPR design with HSE/NII SAPs.
	Fundamental safety overview volume 2: design and safety chapter Q: human-machine interface (no date or reference provided).

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
ECEP060987 Rev A1, February 2007. EDF.	Summary and Results of the FA3 and 4 ETB Ergonomic Study (2006).
ECEMA061033 Rev A1. January 2007. EDF.	PMC (Fuel Handling) System Specification.
ECEIG061187 Issue A1. June 2006. EDF.	Specifications for DN./DS. Systems – Lighting of EPR rooms.
ECEP071048 Rev A. July 2007. EDF.	Procedure For Taking Into Account Human Factors In Fuel Handling Operations.
6474/TR/002. Issue 02 (2010). AMEC.	EDF and AREVA GDA Task Analysis of Example Claim 1: Start-up of the Station Blackout Diesel Generators following a Loss of Offsite Power.
16474/TR/0003. Issue 2 (2010). AMEC.	EDF and AREVA GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims.
16474/TR/006. Issue 01 (2010). AMEC.	EDF and AREVA GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK].
16474/TR/005. Issue 02 (2010). AMEC.	EDF and AREVA GDA Task Analysis: Example Pre-Fault Analysis.
ECEP101809, Rev A. July 2010. EDF.	Human Factors tests for EPR Flamanville 3 in 2009-2010 on the phase 2 simulator.
	EPR – Optimisation of Activities with radiation protection risk RCP, RCV, RIS/RRA, [RCS,CVCS, SIS/RHRS] Valves – Section 1 (2007).
ECEF050543 Ind A. October 2005. EDF.	ENG 3.23.Methodology Guide for Reliability - Maintainability – Availability Analysis.
C45.C.015 EN Rev 00. January 2009. EDF.	Book of Technical Specifications; Valves for Nuclear Power Plants C.015.00.
ECEIG0100625 Rev A. December 2001. EDF.	Procedure MIP EPR No 2.64 Installation Guide – Consideration of Human Factors].
ECEIG070082 Ind A. June 2007. EDF.	Process for Monitoring of Installation Studies and Tracking of PDMS model data modifications, by Building.
ECEIG050365, Ind A. May 2006. EDF.	Monitoring Programme for Sofinel Civil contract.
ECEIG050444 Ind A. November 2005. EDF.	Monitoring Programme for Areva Civil contract YR1401.
ECECC041294 Rev C1. 2005. EDF.	Specification book of layout studies for French EPR MCR, annexes and full scale simulator room.
ECEIG0100002, Rev A1. 2001. EDF.	Layout Rules File – Main Control Room and areas.
ECEIG0100093 Rev A. 2001. EDF.	EPR General Installation Specification Writing Guide.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
CSCT YR5511 CCF 04 Rev E_EN October 2009. EDF.	Technical specifications and conditions, Functional Expression of Need.
ECEF 100427_CCI, Rev A. March 2010. EDF.	An overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards.
Work Stream 4	
UKEPR-0002-181 Issue 4.	PCSR Sub Chapter 18.1 – Human Machine Interface
H-T64-2007-01446-FR Version 01. January 2008. EDF.	Human Factors Programme for Evaluation of the EPR's operating Means Before the 1st Fuel Loading
ECEF012001 Rev A. December 2001. EDF.	Approach for Integration of Human Factors in EPR Design.
ECEF 100427_CCI, Rev A. March 2010. EDF.	An Overview of the Human Factors Approach Used for the EPR Design and Compliance with International Standards.
ND(NII) EPR00169N.	UK EPR – HF Organogram – Topic Meeting Action 1-HF-02.
	Gody, A. (2010) TQ-UKEPR-925 SQEP.
	Gody, A. (2010) TQ-UKEPR-1354 HF training for design engineers.
	Gody, A. (2010) TQ-UKEPR-924 HFI Process.
	Gody, A. (2010) TQ-UKEPR-1026 The application of HF.
ECEP071048 Rev A. July 2007. EDF.	Example of a fuel handling analysis: Taking account of human factors for fuel handling activities.
SFLEFMF 2006.109 Rev. F. 2010. Sofinel.	Fuel Handling System Technical Specifications.
Groupe Permanent Reacteurs (2000).	Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurised Water Reactors.
16474/TR/001. Issue 01 July 2010. AMEC.	EDF/AREVA GDA Task Analysis Method Statement.
ECEF050861/A, Draft, 1 August 2005. EDF.	Graphismes de la Bibliothèque des Objets Graphiques (BOG) du palier EPR » (EPR series graphic object library graphics), report CNEN/FSE.
ECEF050717 Rev A1. 2005. EDF.	Structuring the Requirements and Specifications Concerning the EPR HMI.
ENFCRI090069 Rev. A. March 2009. EDF.	SICS operating principles.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
CSCT YR5511 suite of documents: CCF 01 Rev F CCF 02 CCF 03(b) Rev A1 CCF 04 Rev E CCF 05(b) CCF 05(b) Annexe 1, Rev A1 CCF 05(b) Annexe 8 CCF 05(b) Annexe 9 CCF 06 Rev B1 CCF 06 Annexe 1 Final version CCF 07 Rev B1 CCF 08(a) Rev D1 CCF 08(b) Rev C1 CCF 09 Rev D1 CCF 10 Rev B1 CCF 11 Rev C1 CCF 11 Annexe 1, Rev A1 CCF 12 Rev C1 CCF 13 Rev C1 CCF 14 Rev B1 CCF 15(a) Rev C1 CCF 15(b) Rev B1 CCF 16 Rev C1 CCF 17 Rev C1	Technical specifications and conditions for control and instrumentation systems
ECIG0001089 Rev C1. September 2009. EDF.	Reactor Building Specifications.
ECEIG0000756 Rev C. September 2007. EDF.	EPR – Technical Specifications for the Diesel Buildings.
ECEIG0100002 Rev A1. 2001. EDF.	Sheet C5 Control Rooms and Annexes.
C45.C.015 EN Rev 00. January 2009. EDF.	Book of Technical Specifications: Valves for Nuclear Power Plants.
	Gody A (2010) TQ-EPR-923 Target Audience Description).
DPN/DDAI-PA3E Gody, A. 2010.	Target Audience Description.
	EDF (2010) TQ-EPR-988 OEF.
UKEPR-0002-124 Issue 02. (2009).	PCSR – Sub-chapter 12.4 – Dose uptake optimisation.
ECEP060987 Rev A1, February 2007. EDF.	Summary and Results of the FA3 and 4 ETB Ergonomic Study.
	EDF (2010) EQ-EPR-926 Management of HF Issues.
NEPS-F DC 191, Rev A. January 2010. AREVA.	Human Reliability Analysis notebook of the UK EPR Probabilistic Safety Analysis – Chapter 5.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
54/05/021/A Ind A. 2006. EDF.	EPR computerised operation: protocol for complementary tests HT.
CSCT YR5511 CCF 06 Rev B1 EN. October 2009. EDF.	Technical specifications and conditions - Document CCF 06 Requirements governing dependability Tracking Assumptions – Implementation.
ECEF032026 Rev A1 2003. EDF.	Feasibility Study on Application of DPN Specifications to EPR Computerised Operation – focus on verifying DPN specifications.
HT5403016 Ind A. 2003. EDF.	EPR Computerised Operation: Protocol for Evaluation Tests Relative Operation Department requirements.
ECEF060191 Rev A1. 2005. EDF.	EPR HMI – Evaluation of the Principles of Computerised operation – Assessment of the 2005 Supplementary Test Campaign.
	Gody, A (2010) TQ-EPR-769 Full Response – MCR Manning Levels.
	Gody, A (2010) TQ-EPR-1049 Full Response – Cognitive Workload Assessment.
ECEIG101570 Rev A. 2010. EDF.	Review of the FA3 PDMS model of the installation level +19.50m of the nuclear auxiliary building, June 2010.
ECEIG051259 Rev A. 2005. EDF.	Review of the levels +9.60m to 0.00m for the nuclear auxiliary building.
ECEIG080125 Rev A. 2008. EDF.	Review of the FA3 PDMS model D1 for the levels 0.00m and +3.70m of the nuclear auxiliary building, 16/01/2008 –. No HF presence, but HF issues addressed – hand wheels position too high.
ECEIG080629 Rev A. 2008. EDF.	Review of the FA3 PDMS model D1 for the level +7.40m of the nuclear auxiliary building, 17/04/2008 –. No HF presence, but HF issues addressed – hand wheels position too high.
ECEP071048 Rev A. July 2007. EDF.	Example of a fuel handling analysis: Taking account of human factors for fuel handling activities.
	Gody, A. (2010) TQ-EPR-1027 Supplier HF.
Work Stream 5	
UK EPR-0002-074 Iss. 02 EDF and AREVA, (2009).	UK EPR Pre-Construction Safety Report Principally, Chapters 18.1, 7 (Appendices A and C) and 9.5.
ECEF012001 Rev A. December 2001. EDF.	Approach for Integration of human factors in EPR Design.
CSCT YR5511 CCF 04 Revision E. 2009. EDF.	Technical specifications and conditions - Document CCF 04 Functional expression of need.
ECEF 100427_CCI, Rev A. March 2010. EDF.	An Overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards.
ECEF032026 Rev A1. 2003. EDF.	Feasibility Study On Application of DPN Specifications to EPR Computerised Operation.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
HT – 54/05/021 Ind A. 2006. EDF.	EPR Computerised Operation: Protocol for Complementary Tests.
ECEF060191 Rev A1. 2005. EDF.	EPR HMI - Evaluation of the Principles of Computerised Operation Assessment of the 2005 Supplementary Test Campaign.
H-T54-2007-01446-FR. Version 1.0. January 2008. EDF.	Human Factors Programme for Evaluation of the EPR's Operating Means Before the 1st Fuel Loading.
CSCT YR5511 CCF 08(b) Rev C1. 2009. EDF.	Technical Specifications and Conditions – Conventional Control Systems.
CSCT YR5511 CCF 07 Rev B1. 2009. EDF.	Technical Specifications and Conditions – Automatic Systems.
ECEF 02 1855 Rev. B1. 2006. EDF.	ENG 2.21 Procedure: Degree of Automation for Plant Systems.
UKEPR-0014-001 Issue 00. 2009. EDF.	N4 and EPR Computerised Operation Principles.
ECEF05.0717 Ind A. 2005. EDF.	Structuring of the Requirements and Specifications Concerning the EPR Human-Machine Interface.
16474/TR/0003. Issue 02 September 2010. AMEC.	GDA Task Analysis: Method Statement and Analysis of Two Example Operator Claims.
16474/TR/005. Issue 02 November 2010. AMEC.	GDA Task Analysis: Example Pre-Fault Analysis.
16474/TR/006. Issue 01 December 2010. AMEC.	GDA Task Analysis: Post Fault Example 3 [OP_FEED_TK]
Radiation Protection Topic meeting EDF-CEN Montrouge 15–17 March 2010. Luzeau F., (2010).	Presentation of the 3D-Model of the Flamanville 3 EPR.
ND Meeting, Manchester 18 May 2010. Luzeau F. (2010).	Presentation of the Waste Treatment Building (ETB) for the UK EPR 2 Presentation of the Fuel Building.
ECEIG0100002 Rev A1. 2001. EDF.	Dossier des Règles d'Installation – Salle de commande et annexes.[Layout Rules File – Main Control Room and areas].
ECECC041294 Rev C1. 2005. EDF.	Technical Specifications and Conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scope simulator room of the EPR France Plant.
Powerpoint presentation 21st June 2010 EDF and AREVA. 2010.	General Presentation of the Main Control Room.
ECEF040974 Rev B1. 2006. EDF.	EPR Operations Display Engineering Rule EG 02-34"Display Specification".
ECECC090517 Rev B1. 2010. EDF.	Report on recorded differences between Unit Operator Workstation Panel HMI and simulated Operator Workstation HMI.

Table 14

GDA Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
ECEF021069 Rev C1. March 2008. EDF.	Sizing of SICS.
ENFCR1090069 Rev A. March 2009. EDF	SICS Operating principles.
ECEF 09.1246 SICS (draft). 2010. EDF.	Draft SICS Procedure Incident and Accident - Orientation Initiale
ECEF040683 Rev C1. August 2008. EDF.	ENG 2-33 procedure: Principles for specifying and handling alarms for EPR.
D4002.92-07/084 Rev 01 EN. 2010. EDF.	Guiding Principles Relating to the Organization of the Flamanville 3 Shift Crew.
ECEF060191 Rev A1. 2005. EDF.	EPR HMI - Evaluation of the principles of computerised operation - assessment of the 2005 supplementary test campaign.
ENFCR1090272 Rev A . 2009. EDF.	State Oriented Approach- Designer Knowledge Transfer.
ENFCR1080224 Rev A. 2009. EDF.	SOA- Designer Knowledge Transfer Appendix 1 Plant Review.
ECEF061275 Rev A1. 2008. EDF.	Procedure EPR ENG 3-40: Contents and Structure of Emergency Operating Method.
CSCT YR5511 CCF 03b Rev A1. 2009. EDF.	Technical Specifications and Conditions – Document CCF (03b) Architecture.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-01	The licensee shall ensure comprehensive identification of human based safety claims, and justify the relevance and applicability of the claims to the UK EPR as part of the HRA revision.	4.2.1	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-02	The licensee shall explicitly highlight the human error probabilities associated with Type A HFEs as part of the Level 1 HRA revision.	4.2.1	Prior to Fuel Load.
AF-UKEPR-HF-03	The licensee shall undertake a systematic analysis to demonstrate that all credible Type B HFEs are included in the revised Level 1 HRA.	4.2.1	Prior to Fuel Load.
AF-UKEPR-HF-04	The licensee shall undertake a systematic analysis to demonstrate that all credible Type C HFEs are included in the revised Level 1 HRA.	4.2.1	Prior to Fuel Load.
AF-UKEPR-HF-05	The licensee shall undertake a systematic analysis to demonstrate that all credible HFEs are included in the revised Level 2 HRA.	4.2.1	Prior to Fuel Load.
AF-UKEPR-HF-06	The licensee shall establish and maintain a log of current assumptions from the safety case, including consideration of those identified in Annex 3, Table A3.1. Additional assumptions should be added as they emerge from subsequent HF analysis work. All assumptions shall be substantiated as part of the forward work programme for HF.	4.2.1.1	Prior to First structural concrete.
AF-UKEPR-HF-07	The licensee shall review available HRA methods for the proposed UK EPR HRA revision, in the light of the digital nature of operator interfaces. The choice of HRA method shall be justified as appropriate in line with ND TAG T/AST/063.	4.3.1	Prior to Fuel Load.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-08	The licensee shall justify the HEP values applied for pre-accident task recovery in the light of comments made in the GDA Step 4 HF report, as part of the HRA revision.	4.3.2.1	Prior to Fuel Load.
AF-UKEPR-HF-09	The licensee shall provide information on how the raw data applied to Type B HFE quantifications has been processed, as part of the HRA revision.	4.3.2.1	Prior to Fuel Load.
AF-UKEPR-HF-10	The licensee shall justify the quantitative modelling of error recovery as part of the HRA revision.	4.3.2.1	Prior to Fuel Load.
AF-UKEPR-HF-11	The licensee shall justify the approach for the HRA modelling of diagnostic errors when revising the HRA.	4.3.3.1	Prior to Fuel Load.
AF-UKEPR-HF-12	The licensee shall justify the HRA method applied to the revised Level 2 PSA, and clearly highlight any deviation from its typical and expected application.	4.3.4.1	Prior to Fuel Load.
AF-UKEPR-HF-13	The licensee shall ensure that identical actions are quantified by the same approach in both the Level 1 and 2 PSA HRAs – or alternatively the licensee shall ensure that the HRA methods used for the Level 2 PSA HRA are not optimistic relative to the Level 1 PSA HRA assessments.	4.3.5.4	Prior to Fuel Load.
AF-UKEPR-HF-14	The HRA methods used for OSSA actions in the Level 2 PSA shall be fully justified and ensure qualitative insights are obtained for the development of OSSA guidance.	4.3.5.4	Prior to Fuel Load.
AF-UKEPR-HF-15	The licensee shall calculate the HEPs for initiating human errors based on an analytical process that includes consideration of dependency within the initiator and with other initiating HFEs.	4.3.7.1	Prior to Fuel Load.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-16	The licensee shall provide evidence to support the claims that maintenance and test procedures will minimise the potential for human error dependence.	4.3.7.1	Prior to Fuel Load.
AF-UKEPR-HF-17	The licensee shall justify the assertion of zero dependency within sequences.	4.3.7.1	Prior to Fuel Load.
AF-UKEPR-HF-18	The licensee shall provide evidence of the application of a systematic consideration of coupling mechanisms relating to dependency level allocations within the HRA.	4.3.7.1	Prior to Fuel Load.
AF-UKEPR-HF-19	The licensee shall qualitatively substantiate the dependency levels applied within the HRA.	4.3.7.2	Prior to Fuel Load.
AF-UKEPR-HF-20	The licensee shall identify multiple operator actions within cutsets and reconsider and justify those where the combined HEPs are lower than $1.0\mathrm{x}10^{-5}$.	4.3.7.2	Prior to Fuel Load.
AF-UKEPR-HF-21	The licensee shall provide a comprehensive justification for the allocation of levels of dependence for OSSA actions modelled in the Level 2 PSA.	4.3.7.3, 4.3.7.4	Prior to Fuel Load.
AF-UKEPR-HF-22	The licensee shall ensure that the adequacy of HF maintenance and maintainability requirements is explicitly addressed in their V&V programme.	4.4.2, 4.5.2.2	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-23	The licensee shall ensure that the system and equipment design specifications contain a detailed set of HF requirements and are based on recognised standards where appropriate.	4.4.2, 4.5.2.2	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning
AF-UKEPR-HF-24	The licensee shall develop and submit a HFIP for UK EPR construction.	4.5.1	Prior to First structural concrete.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-25	The licensee shall ensure that sufficient SQEP HF resource is identified and deployed to meet the demands of the on-going design and safety case work for the UK EPR.	4.5.2.1	Prior to First structural concrete.
AF-UKEPR-HF-26	The licensee shall produce a user definition document that contains relevant anthropometric details and has considered the impact of secular trends in the operating community.	4.5.2.2	Prior to First structural concrete.
AF-UKEPR-HF-27	The licensee shall establish and maintain a consolidated HF Issues Register for the future design and safety case development beyond PCSR. This will incorporate all outstanding HF Issues and requirements that have arisen from the work to the end of GDA.	4.5.2.2	Prior to First structural concrete.
AF-UKEPR-HF-28	The licensee shall ensure that there is full integration between the remaining HFE programme, the HRA and the overall safety case,	4.5.2.2	Prior to First structural concrete.
AF-UKEPR-HF-29	The licensee shall establish a process for addressing ALARP requirements for HF aspects of the design and safety case for the UK EPR.	4.5.2.2	Prior to First structural concrete.
AF-UKEPR-HF-30	The licensee shall design the UK EPR workstations to accommodate the UK user population, based upon reasonable estimates of the secular trend. The anthropometric data applied shall be justified.	4.6.2.1	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-31	The licensee shall provide justification and evidence of the suitability of the workspaces and working positions in the UK EPR (not limited to the MCR) for the UK working population.	4.6.2.2	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-32	The licensee shall provide further information on and justification relating to the emergency lighting design and relevant plant-wide minimum lighting levels.	4.6.3	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-33	The licensee shall undertake detailed analysis of the thermal environment in the MCR and RSS and provide justification of its applicability for the full range of conditions envisaged for operations from each location.	4.6.3	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-34	The licensee shall verify that the target noise levels have been met as part of the V&V of the UK EPR.	4.6.3	Prior to Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-UKEPR-HF-35	The licensee shall produce the detailed design and justification of the human machine interfaces for the UK EPR.	4.6.4, 4.6.4.1	Prior to Fuel Load.
AF-UKEPR-HF-36	The licensee shall provide a HMI style guide (or equivalent); using recognised modern standards to guide detailed design and justification of the interfaces and displays for the UK EPR.	4.6.4.2	Prior to First structural concrete.
AF-UKEPR-HF-37	The licensee shall ensure that PICS functional degradation is alerted to the operators.	4.6.4.2, 4.6.5.1	Prior to Fuel Load.
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.	4.6.4.3	Prior to Fuel Load.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-39	The licensee shall provide a justification and evidence of the visibility of the detailed POP displays proposed for the UK EPR.		Prior to Fuel Load.
AF-UKEPR-HF-40	Assessment Finding AF-UKEPR-HF-40 – The licensee shall justify the design of the hard wired OS/OA panels for the UK EPR	4.6.4.4	Prior to Fuel Load.
AF-UKEPR-HF-41	The licensee shall undertake detailed design and justification of the SICS panel for the UK EPR.	4.6.4.4	Prior to Fuel Load.
AF-UKEPR-HF-42	The licensee shall undertake detailed analysis and justification of the implementation of the PICS in the RSS to ensure that all required operations can be achieved.	4.6.4.5	Prior to Fuel Load.
AF-UKEPR-HF-43	The licensee shall justify the design of the audible alarm signals for the UK EPR.	4.6.4.6	Prior to Fuel Load.
AF-UKEPR-HF-44	The licensee shall demonstrate that a consistent approach to alarm prioritisation and configuration is taken throughout the UK EPR.	4.6.4.6	Prior to Fuel Load.
AF-UKEPR-HF-45	The licensee shall set a maximum rate of alarm activation in the UK EPR alarm design specification	4.6.4.6	Prior to Fuel Load.
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.	4.6.4.6	Prior to Fuel Load.
AF-UKEPR-HF-47	The licensee shall explain and justify the reliance of any manual actions on response to alarms during SOA operation.	4.6.4.6	Prior to Fuel Load.
AF-UKEPR-HF-48	The licensee shall justify the design of procedures for application on the UK EPR.	4.6.5.1	Prior to Fuel Load.

Annex 1

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

Human Factors – UK EPR

Assessment Finding Number	Assessment Finding	Report Section reference	Timescale
AF-UKEPR-HF-49	The licensee shall substantiate that the SOA procedures ensure that claimed safety actions are reliably completed within the timescales required by the safety case.	4.6.5.1	Prior to Fuel Load.
AF-UKEPR-HF-50	The licensee shall ensure that the PICS continuously displays an appropriate overview to support implementation of the selected SOA during SOA operation or a justification as to why this is not reasonably practicable.	4.6.5.1	Prior to Fuel Load.
AF-UKEPR-HF-51	The licensee shall justify the design of the SICS panel and the administrative controls relating to transfer from PICS to SICS.	4.6.5.1	Prior to Fuel Load.
AF-UKEPR-HF-52	The licensee shall validate the entire suite of MOP for the UK EPR.	4.6.5.2	Prior to Fuel Load.
AF-UKEPR-HF-53	The licensee shall substantiate the proposed manning levels and organisational structure for the UK EPR.	4.6.6	Prior to Fuel Load.
AF-UKEPR-HF-54	The licensee shall analyse and substantiate the workload levels for UK EPR MCR operators.	4.6.6	Prior to Fuel Load.

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

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

Annex 2

GDA Issues – Human Factors – UK EPR

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

IDENTIFICATION AND 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 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

IDENTIFICATION AND 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 2

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.		

Further explanatory / background information on the GDA Issues for this topic area can be found at:	
GI-UKEPR-HF-01 Revision 0	Ref. 155.

Annex 3

Work Stream 1 Supporting Analysis

Introduction

1 This annex presents further details of my Work Stream 1 assessment. This includes:

- Tabulation of the explicit and implicit assumptions made by EDF and AREVA.
-
- Details of my assessment of the four example Task Analyses submitted as part of EDF and AREVA's forward action plan.

It is important to note that this annex presents the findings at the time of the individual task analysis assessments. As a result of the third task analysis, EDF and AREVA concluded that the proposed methodology for the pre-fault Type A *HFEs* required amendment and have since submitted a revised approach. I will assess this as part of my post-Step 4 Assessment Report. Additionally my findings in Section 4.2 of the main report present those that I have judged to be appropriate for Step 4 GDA, i.e. those appropriate to a PCSR stage.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
Explicit Assumptions		
Assumptions concerning Design/Operations		
Procedures will minimise dependency.	It is asserted that some dependency (e.g. dependency between pre-initiator actions) will be controlled by optimal procedures. There is insufficient discussion of how this will be assured.	I am unable to determine whether all dependencies have been suitably considered.
MCR will be designed in accordance with international good practice and hence will provide an optimal environment.	Whilst it is expected that the MCR will be designed in this manner, there is insufficient discussion of how some of the novel features of UK EPR (e.g. SOA, auto-diagnostics) will be optimised.	I am unable to determine whether there are claims made on operators arising from the use of Automatic Diagnosis (AD) and SOA that need explicit consideration.
OEF is a valid basis for the identification and assessment of *HFEs.*	Whilst operating experience is an important input to the process of identification and assessment of *HFEs*, there is insufficient justification for why experience on previous reactor types will be relevant to UK EPR, and how the differences might affect the application of that experience.	The use of OEF has been at a high level and the differences between the sources of OEF and UK EPR have not been made sufficiently clear, and hence I cannot identify whether all relevant *HFEs* have been considered.
HEP of 1.0×10^{-1} assumed for prevention of flooding.	This appears to be used as a conservative screening value.	I have not found analysis of relevant *HFEs* and therefore cannot confirm completeness.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
HEP of $1.0\text{x}10^{-2}$ for failure to extinguish fire in MCR.	It is unclear whether this assumes that all fires are capable of being extinguished. It does not consider the potential for operators to fail to evacuate in good time (i.e. they remain and attempt to fight the fire for too long).	I have not found analysis of relevant *HFEs* and therefore cannot confirm completeness.
Conservative assumptions have been made with respect to recovery from pre-initiating *HFEs* (only manual valve operations).	The assumption is that only a single recovery is claimed. In the absence of detailed modelling it is not clear that the opportunity is being taken to improve the design of maintenance and other tasks.	I have not found analysis of relevant *HFEs* and therefore cannot confirm completeness.
It is assumed that non-recovery following incorrect action (but correct diagnosis) is very unlikely.	Clarification is required as to whether this is assumed to be zero, or whether a level of unrecovered incorrect action is modelled.	There may be *HFEs* that increase the likelihood of non-recovery. The nature of the claimed *HFEs* associated with recovery needs to be made explicit.
Human Performance Limiting Values (HPLV) have been applied to *HFEs* to address non-modelled dependencies.	The absence of detailed task analysis means that it is not clear whether such an approach is sufficient.	I cannot determine whether dependencies have been adequately considered.
Severe accident response is based on OSSA.	There will be a need to demonstrate how OSSA integrates with the State Oriented Approach.	I have not identified analysis that makes clear the set of *HFEs* that will affect performance of OSSA.
Assumptions Concerning Substantiation Process		
Suitability of ASEP for L1 PSA.	The suitability of ASEP for this application is being considered in WS5.	WS5 Assessment refers.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
There is no dependency between pre-initiator *HFEs* and post fault *HFEs*, nor between different pre-initiator *HFEs.*	The assumption concerning pre-initiator and post-fault *HFEs* is reasonable, but requires substantiation. The justification for the assumption concerning different pre-initiator *HFEs* is less clear.	The claim that there is no dependency needs to be substantiated.
Probabilities for false diagnosis are based on ASEP (i.e. not modelled explicitly).	It does not appear that there has been detailed examination of the potential for false diagnosis, and hence it is unclear to what extent the time for successful completion of tasks, or the ability to recover from mis-diagnosis, is reasonable.	I consider the analysis of misdiagnosis errors to be incomplete.
Actions within the MCR can be commenced within 5 minutes of initial indication.	I consider this to be a reasonable starting point given the nature of the MCR and the manner in which actions are undertaken. However, as revealed by TA4, I do not consider that there has been sufficient substantiation of the MCR philosophy that removes the requirement for responding to alarms (other than the AD alarm) once the SOA has been entered. It makes implicit assumptions concerning manning levels that need to be carried forward to the Licensee manning arrangements.	I consider that the assumption may mask certain potential shortfalls, and hence that further analysis is required.
An HEP of 5.0x10^{-2} has been assumed for incorrect action following correct diagnosis, based on previous PSA.	For action in the MCR this may be reasonable, but it makes implicit assumptions concerning the design of the interface that need to be justified. This generic HEP may not be appropriate for incorrect action Local-to-Plant.	I do not consider that the PICS has been sufficiently substantiated with respect to the HMI and the operator-system dialogues.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
Any Performance Shaping Factor (PSF) that has not been modelled explicitly is assumed to have a zero effect (i.e. neither increases nor decreases the HEP).	This is based on an assumption that the plant will be designed in accordance with recognised good practice. It also assumes, however, that all relevant PSFs have been recognised, whereas the absence of detailed task analysis makes it difficult to judge whether this is correct.	I consider that further analysis of tasks is required to assure this claim, particularly with respect to aspects of the MCR that are new to UK operations.
The Emergency Organisation will be designed in accordance with good practice, and will be provided with a favourable task environment.	The design of the Emergency Organisation will need to be substantiated.	The current level of substantiation is incomplete, particularly with respect to the RSS.
For Level 2 PSA, basic HEPs of $1.0\text{x}10^{-2}$ for diagnosis and $1.0\text{x}10^{-3}$ for response have been assumed, with recovery actions as part of the HEP derivation.	This will need to be substantiated.	These assumed HEPs require substantiation as they cannot be considered screening values.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
Implicit Assumptions		
Assumptions Concerning Design/Operations		
The roles of staff within the MCR support error recovery.	This also makes claims on situation awareness and on team performance that require substantiation.	*HFEs* associated with the team roles are not made explicit, particularly with respect to recovery actions.
Operators have sufficient understanding of the process logic so that they can apply the initial orientation procedures to support the initial diagnosis.	This makes claims on operator training and competence that should be made explicit.	The potential for *HFEs* associated with commission errors is not made explicit.
Operators will respond to the alarm system in a timely manner.	The alarm system, including auto-diagnostics, requires substantiation if there is to be confidence that operators will be able to respond in a timely manner to initial indications of process disturbance.	There is incomplete analysis of the potential *HFEs* that would affect mis-diagnosis.
The use of the Auto-diagnostics is mandated within the operating concept for UK EPR.	The impact of the operating philosophy comprising the use of AD is not modelled.	*HFEs* associated with the use of AD have not been modelled explicitly.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
The staffing philosophy (Operator-Action, Operator-Strategy, Supervisor, Safety Engineer) is implicit in the documentation submitted.	The implications of this staffing structure in respect of *HFEs* associated with post-fault actions is not made explicit.	I cannot determine whether the proposed operating philosophy might generate novel *HFEs*.
Assumptions Concerning Substantiation Process		
The design of the PICS provides adequate support for Situation Awareness.	Implicit claims for recovery from incorrect diagnosis or incorrect action rely on the use of the PICS and the State Oriented Approach. This requires substantiation.	I consider that there has been insufficient analysis of the role of the PICS and the MCR organisation in defending against mis-diagnosis.
The mandated use of the auto-diagnostic module does not reduce the ability of the operator to challenge the guidance from the auto-diagnostics.	Any claims that the operator will be able to detect and respond to an error in the auto-diagnostic guidance will require detailed substantiation.	I do not consider that there has been sufficient analysis to demonstrate that operators will be able to detect and respond to AD errors and failures.
The State Oriented Approach will support the operator in identifying required actions.	The modelling of post-fault actions assumes that indications of required actions are clear, unambiguous and timely, and that the SOA guidance is correct. This requires substantiation.	I consider that further detailed substantiation is required for a range of post-fault actions supported by SOA.

Annex 3

Work Stream 1 Supporting Analysis

Table A3.1: Explicit and Implicit Assumptions

Assumption	Comment	Completeness
Operators will be able to use the Safety Instrumentation and Control System (SICS) in an appropriate manner.	The use of the SICS panels, both for monitoring actions via PICS, and for response following failure of PICS, requires substantiation.	I have not identified any detailed substantiation of the use of SICS.

Annex 3

Work Stream 1 Supporting Analysis

Example 1: Post-Fault Error (SBO Diesels)

2 This task was selected by EDF and AREVA for detailed analysis as it scored highly both for FV and RIF (both within the top 20 *HFEs*). The task is OP_SBODG2H, comprising manual start of the Station Black-Out (SBO) Diesel Generators within two hours. The HEP identified for this task is 2.1×10^{-3}.

3 I identified a set of comments based on the initial submission of the Task Analysis (TA) (Ref. 41). I have amended these comments in the light of the revised TA1 submitted together with TA2 (Ref. 42). The numbering refers to the paragraphs in the revised TA (Ref. 42).

4 My comments fall into two sets, being those that relate to how the example illustrates the generic method, and those that relate to the specific task. The first set concerns the specific TA. Where the comments have generic implications for the method this is noted subsequently.

<u>SBO Start-up Assessment</u>

5 3.1 - The declared scope comprises a qualitative assessment of the claim. This is necessary but not sufficient for substantiation.

6 I am unclear what the relevant operating experience of the staff was who supported the analysis.

7 The declared objectives of the analysis do not appear to me to fully match those set out in the Method Statement, including demonstration of the appropriateness of the operation being carried out by an operator.

8 The need to form a judgement concerning the quantitative assessment (HEP) used within the PSA should be a part of the process reported within this document, rather than being a subsequent activity, as I consider the insights gained by the analysts to be essential for a valid quantitative assessment.

9 4.1 - I do not consider the selection of this task for assessment to be sufficiently clearly explained within the document. In particular, the reasons for selecting this task rather than other similar ones should be justified (e.g. OP_SBODG15M, OP_SBODG30M). Its selection based on Fussell-Veselv (FV) or RIF should be explained. The boundaries of the task should be further explored to consider concurrent tasks and activities and precursor activities.

10 4.3 - I note that the attempted start-up of the EDG is undertaken in parallel with the claimed task, whereas the TA itself appears to require these actions to be sequential and the subsequent discussion within the document notes the apparent ambiguity. Although the revised TA has clarified that the Local-to-Plant actions are not required, there needs to be clarity within the TA concerning the assumptions associated with sequencing of actions if the TA is to be considered valid.

11 4.5 - The existence of the previously assessed HEP is noted. The value of the HEP has been provided and a judgement made within this document concerning its validity. I note that Section 4.17 identifies caveats concerning the validity of the HEP.

12 4.6 - The different personnel within the MCR is noted, together with brief comment on the interactions between them. However, the HTA does not explicitly address the different

Annex 3

Work Stream 1 Supporting Analysis

roles and there is no consideration of interactions and communications between the staff. Whilst it is claimed that the OA undertakes all the actions, the benefit of the other staff for error recovery is noted and hence their interactions are relevant.

13 It is noted that the OA and OS sit at adjacent desks with access to the same interfaces and paper-based incident procedures. This statement is ambiguous. I am unclear whether the two operators use the same paper-based procedures, or whether they use different procedures, as was indicated when I visited the simulator in June 2010. It is also stated that the OS does not monitor actions defined in the MOP. The role of the OS needs clarification, as I understood that they do fulfil a monitoring role – and hence the nature of the monitoring should be explained.

14 Whereas it is correct that the actions by Field Operators (FO) local to plant are not part of the claimed action, as noted above it is important to clarify the sequencing with respect to attempted start of EDG and hence to consider the demands on the OA associated with the process of attempted start of EDG (e.g. communication with FO).

15 4.8 - The HTA considers key task steps relating to the specific claimed action. However, it does not consider other concurrent tasks that might affect the claimed action. Nor does it consider different roles and communications demands. This is considered a limitation of the HTA.

16 The HTA clearly indicates that EDG start-up is attempted before commencing SBO start-up. Furthermore, it notes that EDG start-up comprises both recognising that they have failed to start and attempting both remote and local start-up.

17 The Level 2 PSA notes that the claimed action includes closing the breakers following SBO start-up. This is not included in the HTA.

18 4.9 - The precise nature of the indications of loss of 10kV should be given, in order that a judgement can be made concerning their adequacy and confusability. The TA notes that there is no unambiguous indication.

19 4.9.1 - The initial TA included comments concerning the use of confusion matrices for diagnosis or misdiagnosis assessment when operating from the conventional alarm panels. The approach appears to have been discounted by EDF and AREVA in the context of screen-based displays, whereas I consider that a similar approach is appropriate as a means of confirming that the AD presentation cannot be misinterpreted. Given the apparent claim that is made for the reliance on the AD indications, such an assessment would be valuable. A screenshot of the relevant AD indications would be beneficial.

20 It is noted that the IO procedures requires the OA to check for relevant alarms. This is a further reason for making explicit the potential confusability of indications at this stage.

21 4.9.2 - Response implementation appears to be reliant on the validity of the AD indications via the PICS. Whereas the indication that the AD has made a diagnosis is clear and unambiguous, it is not clear from the TA whether the indication of the nature of the diagnosis also is sufficiently clear and unambiguous.

22 It is stated that there is currently no PICS status display to support the operator and the need for one is noted in HFIR003. No guidance is given concerning the nature of the errors that could arise in the absence of such a display and hence the information that

Annex 3

Work Stream 1 Supporting Analysis

needs to be incorporated into such a status display to reduce the likelihood of such errors.

23 Screenshots of the cited PICS screens would be valuable (e.g. KAE 5010 YE, ~3501 YE, ~3801 YD and 3LJP/LJS 0001 YC.

24 No information is provided within the TA document to indicate the nature of potential navigation errors when moving between screens. It is therefore not possible to form a view of their likelihood or consequence, nor of how they would be revealed and the ability to recover from them.

25 4.10.1 - It is stated that the OS monitors the OA's progress through the IO procedure and hence provides a recovery mechanism. The nature of this monitoring should be made more explicit and represented within the HTA and, if necessary, the TTA.

26 4.10.2 - A similar comment as 2.10.1 applies, although EDF and AREVA note that the manner in which roles and responsibilities support error recovery is undefined.

27 4.10.3 - The benefit of clear roles and responsibilities is claimed, but there is insufficient supporting analysis to demonstrate this.

28 4.11 - I consider the absence of any quantification of the effects of PSF to be a shortfall in the overall analysis although I note that it is outside the declared scope of the analysis. However, generally the identified PSF are valid and appropriate.

29 4.11.1 - Judgement of adequacy of time is dependent on resolving the ambiguity with respect to EDG.

30 4.11.4 - Whereas it is stated that alarm patterns do not need to be interpreted, the requirement to check for relevant alarms is acknowledged. The TA does not provide sufficient clarity concerning the nature of the task of checking relevant alarms, nor the opportunity for error within this process.

31 4.11.9 - The extent to which the TA process has identified areas where the procedures require enhancement is welcomed. EDF and AREVA should identify what generic issues can be taken from these observations that can be extended to the review and development of all of the UK EPR procedures.

32 4.11.10 - The need to address identified HMI issues within the ongoing programme of simulator design and development is stated. EDF and AREVA should identify what generic issues can be taken from these observations that can be extended to the review and development of all of the UK EPR procedures.

33 4.11.11 - The importance of work organisation and allocation of roles is stated, although the TA does not represent or address this issue. EDF and AREVA should clarify how this will be taken forward.

34 4.12 - The manner in which the timeline analysis has been developed is not clear. In particular, there is insufficient information concerning the levels of uncertainty within each estimate. The task of attempting to start the EDG does not appear to be identified explicitly.

35 There is no attempt to consider the effect of potential errors, such as navigation errors, when negotiating the PICS HMI and their impact.

Annex 3

Work Stream 1 Supporting Analysis

36 There is no explicit consideration of any other tasks and activities that may be required concurrently, or which the operating staff may attempt to undertake concurrently.

37 It is assumed that both OA and OS are present at their desks at the start of the LOOP.

38 4.15 - A number of specific OEF items are noted. Some have been transferred to the HFIR. It should be made explicit if the others are not to be taken forward.

39 3.0 - It is judged that the conclusions are not fully substantiated by the TA as there remains uncertainty concerning the completeness of the HEI process, particularly with respect to navigation and HMI issues and the basis for the TLA requires amplification. The absence of an assessment of the previously derived HEP is considered a gap.

Specific TTA comments (numbers refer to the TTA references):

40 2.1.2 - It is unclear how the declaration of a station incident might then affect workload within the MCR.

41 2.1.3 - Situation awareness is cited as a recovery mechanism, but there is insufficient discussion of how SA is fostered and maintained, or how it might be undermined.

42 2.2.1 - This is an example of where the consequences of the potential errors are noted as ‘unable to complete’, ‘delay’ and ‘potential aggravation by erroneous operation’. Whilst these capture the potential consequences, there is insufficient attempt to consider how this will affect the timeline and, in particular, the likely duration before error detection and recovery. Some assessment of the potential for error and hence the uncertainty associated with the estimated duration would be beneficial.

43 2.2.4 - The uncertainty concerning sequencing is stated. It is stated for the purpose of the TA that the OA continues with the SBO start-up in parallel with the FO attempting to start the EDG. The potential impact of these parallel activities, if any, should be considered in addition to the time required to brief the FO and this should be stated explicitly.

44 3.3.2 - It is unclear whether this task step includes closing breakers, once the SBO Diesels have been started and hence whether this represents the completion of the task.

Generic Issues

45 Generally, the example TA provides confidence that the method will address many relevant issues.

46 From the first TA example, it is unclear to what extent the process is able to consider situation awareness and its role in supporting error identification. Although situation awareness is cited within the TTA as a recovery mechanism, there is insufficient assessment of how SA is fostered and maintained by the SICS and other information within the MCR, nor how the different staff within the MCR interact to facilitate this. Similarly, it is unclear to what extent the process is able to make explicit any errors associated with HMI navigation and format/control selection.

47 The Method Statement does not present a detailed approach to considering diagnostic errors and the use of confusion matrices or similar approaches. The first example TA has dismissed the use of confusion matrices in the context of misdiagnosis for this TA, due to the availability of the auto-diagnosis functionality. Notwithstanding the implicit claim on the AD system, which may need further substantiation, this stance ignores the potential

Annex 3

Work Stream 1 Supporting Analysis

value of an approach similar to confusion matrices for considering error identification and recovery (e.g. after operator error using the HMI, navigation errors, etc).

48 The TA has noted the different roles within the MCR, but has not provided sufficient analysis of the actions of each person and the interactions between them. In particular, the role of the SE is noted but there is little explicit consideration of how SICS indications might influence decisions (particularly for error recovery). The lack of available information concerning the use of SICS is recognised and it may that what is required at this stage is clarity of assumptions.

49 There is a brief reference to the role of the OS in monitoring the OA actions, but no explicit analysis.

50 There is no consideration within the HTA of how the different roles interact, nor of concurrent other tasks that might affect performance of this task.

51 There is no consideration within the TA of how operations prior to the claimed action (in this instance, prior to LOOP) and other actions associated with the initial response to the event (LOOP) might affect situational awareness and hence the ability to respond, or the potential for error.

Example 2: Post-Fault Action (Operator Initiated Cooldown)

52 This task was also selected by EDF and AREVA for detailed analysis as it scored highly both for FV and RIF (both within the top 20 *HFEs*). The task is OP_FSCD_30MN, comprising initiation of cooldown from the MCR following a small-break LOCA, with Medium Head Safety Injection (MHSI) unavailable. The HEP identified for this task is $4.3x10^{-2}$.

53 My comments fall into two sets, being those that relate to how the example illustrates the generic method and those that relate to the specific Task.

54 The first set concerns the specific TA. Where the comments have generic implications for the method this is noted subsequently. My comments on the method do not repeat those made for the previous TA.

Specific TTA comments (numbers refer to the TTA references):

55 5.2 - The initial analysis by EDF and AREVA has revealed that the Event Code is incorrect, as the requirement to initiate Fast Secondary Cooldown (FSCD) within 30 minutes is not credible or required. EDF and AREVA notes that the requirement is to initiate cooldown at 50^{o}Ch-1 and this is what has been modelled. The method is the same, but FSCD is only initiated in response to a subsequent re-diagnosis from the AD and this would be after 30 minutes has elapsed. I note that this suggests that a more detailed analysis of all actions claimed within the HRA Notebook may be required, in order to validate them.

56 5.6 - There is a statement that the OS provides a recovery mechanism for errors by the OA and that the OS does monitor OA actions in accordance with the paper-based procedures, but does not monitor actions defined in the computerised Manual Operating Procedures (MOP). I am unclear whether this means that the OS does not use the MOP for monitoring, or does not monitor any actions described in the MOP.

Annex 3

Work Stream 1 Supporting Analysis

57 5.9.1 - EDF and AREVA notes that the fault scenario diagnosis is automated through the AD system. I consider it important to be clear that the AD does not diagnose the fault scenario. It identifies the required operator actions. EDF and AREVA claims that there is no requirement for the operator to diagnose the scenario. It is unclear to me, however, whether the operator may attempt to diagnose the scenario and whether this might affect their interaction with the AD.

58 5.9.2 - The TA identifies a number of critical PICS formats, and notes their role in supporting *"diagnosing the requirement for [action]"*. I would expect to see a detailed analysis of the interaction with the format, the HMI dialogues, etc. but I have not been able to find this level of analysis, particularly with respect to potential errors. I have noted some navigation-related errors have been identified and recorded on the assumptions register, but I am unclear as to the level of systematic HEI.

59 5.10.1 - The role of the OS as a diverse check on the actions of the OA is noted in the TA. It is not clear to me what the potential dependencies between the two operators are and between the OA/OS and the SS. The use of different procedures between OA and OS should reduce dependency, but it is noted that they use the same information displays. There is no discussion of potential dependency, although the OS is claimed as a potential recovery route.

60 The importance of the PICS status displays for supporting the necessary diagnosis required to identify the need to implement cooldown is noted in the TA, but there appears to me to be little detailed analysis of the potential to misinterpret the status displays.

61 5.11.2 - Time pressure is noted as being absent due to the lack of an explicit requirement, although the likelihood that operators will be aware of the time constraints is also noted. However, no attempt appears to have been made to consider how this trained knowledge might affect performance.

62 5.11.5 - The TA report notes that, because the key indicators are all provided within the main PICS status displays for this scenario, the analysis assumes that the HMI does not constitute a negative PSF. I consider this level of analysis to be insufficient, given the reliance on the HMI. It also does not offer opportunity to optimise the HMI further.

63 5.11.6 - There is a brief mention of the lack of potential for increased workload arising from concern over workers being in the affected plant areas. At the same time, the report does note the potential for distraction to cause an increase in MCR workload. I do not consider this level of workload analysis to be sufficient, given the importance of MCR responses to the scenario.

64 5.11.7 - An assumption has been made concerning the level of training required to ensure that operators understand the need to implement cooldown expeditiously. This assumption appears to me to be reasonable. However, I am unclear how the assumption is to be captured and fed forward to the licensing phase. Furthermore, this appears to me to be in conflict with the assertion referred to in 5.11.2 concerning a lack of time pressure as a consequence of no explicit reference to time windows.

65 5.11.10 - The TA report notes that the functions of some PICS icons are not obvious. This further reinforces my view that a detailed assessment of the HMI is required as part of the substantiation of MCR tasks.

Annex 3

Work Stream 1 Supporting Analysis

66 The analysis provided in this TA report does not appear to consider the potential for, likelihood of, or means of recovery from inadvertent HMI navigation errors. There is a statement that mis-selection of a hyperlink would be a self-revealing error as the format that appeared would not contain the expected information. I consider this to be an unsubstantiated assumption as I could not find analysis that considered whether an incorrect format would always be sufficiently compelling. I consider that such analysis is a necessary part of the evaluation of such HMIs.

67 5.14.1 - I am unclear how the assumptions noted in this paragraph will be clearly fed forward to the licensing phase. The assumptions do not appear to be recorded on the assumptions register.

<u>Methodology Assessment</u>

68 5.9.2 - Reference to the relevant PICS displays is helpful, given the importance of these displays for operator actions, but the absence of screenshots of the displays restricts my ability to evaluate the analysis.

69 The lack of detailed HEI for HMI-level analysis appears to me to be a shortcoming in the implementation of the method, given the level of reliance on the HMI, although I do note that some HMI-related errors have been identified and recorded on the assumptions register.

70 5.11 - The preliminary TA identified that the time available to undertake the task was insufficient, and hence the task could not be completed successfully. As a consequence, no further analysis was undertaken, which I consider to be unfortunate as it means that the opportunity to identify further issues in respect of the task has been lost.

71 5.15 - The keyword search of NUPER and other OEF sources appears to have been limited to those events relating to the initiating event or fault scenarios, rather than to evidence of similar *HFEs* and failure opportunities. I consider that this may have reduced the opportunity to identify OEF that is relevant to the *HFEs*, although I do note that one example OEF item was generic and concerned post-fault procedures and change management failures. I am unclear how this particular event has informed the task analysis.

72 6.2 - In reviewing the methodology, EDF and AREVA observes that a significant number of OEF events were identified. They also note that many of these related to pre-fault human errors. This provides further evidence of the importance of a sufficient analysis of Type A errors.

73 6.4 - The use of Confusion Matrices for understanding fault diagnosis when alarm patterns are to be interpreted is noted by EDF and AREVA. Their use is therefore not considered by EDF and AREVA to be relevant for scenarios where AD is available. I am unclear whether Confusion Matrices or similar approaches might be of value for examining error recovery, particularly in the context of HMI-related errors. I would expect to see a more systematic approach to such analysis.

Annex 3

Work Stream 1 Supporting Analysis

Example 3: Pre-Initiator Action (Pump Maintenance)

74 This task was also selected by EDF and AREVA for detailed analysis as it represented an example of a task that could generate a Type A error (human errors that contribute to the unavailability of the safety systems that might mitigate a fault scenario).

75 Maintenance of the EBS Pumps was selected for analysis as the EBS exceeds the risk screening threshold. EDF and AREVA has determined that the threshold is for a RIF greater than 2 or an FV value greater than $5x10^{-3}$.

76 My comments fall into two sets, being those that relate to how the example illustrates the generic method and those that relate to the specific Task. The first set concerns the methodology.

Methodology Assessment

77 3.2.3.1 - I do not consider that the proposal to use existing conventions and to be consistent with boundaries within the PSA is appropriate, as by doing so they may not fully capture potential human interactions (such as might arise during maintenance on adjacent systems). A HF based approach to defining system boundaries would be beneficial.

78 3.2.3.2 - The ability to identify critical tasks is dependent, in part, on the boundaries that are set and hence the identification of tasks that may affect a particular system. It remains unclear whether the revised approach addresses the original query. Although recovery mechanisms are noted in the proforma (Appendix F of the submission), it remains unclear whether the identification of recovery mechanisms is used to constrain further analysis and, if so, how the adequacy of those mechanisms is judged.

79 App C - Appendix C has been modified to reflect the specificity of pre-fault actions assessment. This has been achieved by removing some of the items previously included. Timeline analysis may continue to be valuable in the context of time pressures as a PSF, as would consideration of allocation of function in the context of whether certain tasks could/should be automated to remove the potential for error.

Task Analysis Assessment

80 1.1 - ND requires a suitable and sufficient Safety Case which takes proper account of HF, not an HF Safety Case. Furthermore, the Safety Case should be consistent with the expectations embodied within the SAP, rather than addressing the SAP.

81 1.4 - The five steps acknowledge that definition of boundaries and identification of tasks are critical steps. It is not clear to me that the method provides an appropriate basis for decisions associated with these steps (see below).

82 1.5 - The method statement is described as being designed to be implemented at a systems level. It is not clear to me that piloting at the equipment level was necessary, or helpful, as it has affected the ability to demonstrate an effective method for considering system boundaries. It is also, therefore, unclear to me whether the method does work at a systems level.

83 The exclusions (e.g. isolation/de-isolation) may be significant tasks. I am unclear whether these exclusions were for the benefit of the pilot analysis, or are considered part of the normal process.

Annex 3

Work Stream 1 Supporting Analysis

84 I am also unclear whether the focus at the equipment level has resulted in lack of consideration of other critical tasks (e.g. other tasks that could affect EBS Pumps, other systems that could be affected by the EBS Pump activities, concurrent tasks that may interact).

85 3.1 - It is noted that the objective of the workshop was only to identify critical tasks rather than to provide a comprehensive error identification process. However, the equipment-based approach results in an inability to consider whether other activities adjacent to the EBS Pumps might affect them. For example, during normal operations (Node 1), adjacent maintenance might affect the EBS Pumps. Similarly, activities in Node 2 (preventive maintenance) might affect other adjacent systems and hence be critical for other systems. This example therefore does not fully demonstrate the ability of this approach to identify all critical tasks nor, in particular, to identify any tasks not already considered in the PSA.

86 There is no indication of the information that would be expected to be available during the Hazard and Operability Study (HAZOP) workshop. In addition to plant and equipment information, operating principles and procedures would be expected to be provided (if available) and OEF would normally be reviewed prior to the workshop. It is not clear what information, if any, was available or is expected to be available for future workshops.

87 The use of the Human HAZOP process only to identify critical tasks (i.e. to stop once a task is deemed critical) loses the opportunity to utilise the Human HAZOP process to inform the TA and HEI activities.

88 3.2 - I am unclear why the related components of the system have been excluded from the analysis (as discussed above).

89 It is noted that planned maintenance takes place during plant shutdown. It is therefore important to consider concurrent activities undertaken during a shutdown.

90 3.4 - I am unclear whether it is intended to use other sources of OEF information in addition to NUPER data, or whether NUPER was used for illustrative purposes. It is noted that the maintenance SME provided additional anecdotal OEF, which illustrates the importance of a broad set of OEF sources.

91 3.5 - I am unclear whether the HTA represented in Figure 2 was derived prior to the Human HAZOP workshop, or whether the reported consistency was indicative of the comprehensive nature of the workshop.

92 There does not seem to be any functional testing/return-to-service checks identified under planned maintenance, which would provide recovery opportunities. It is therefore unclear whether this is an artefact of the decision to exclude plant isolation/reinstatement. Such functional checks should be considered as part of the overall maintenance activity.

93 3.6 - A number of inspection activities have been deemed non-critical because a failure of inspection is considered not to introduce an additional latent failure mode. Rather, it comprises a failure of a recovery mechanism for an existing latent failure. This is acceptable only if no claims are made for routine inspection when considering hardware reliability rates. Given that such rates tend to be derived from operating experience, it is important to be clear whether such inspections are implicit in those failure rates.

Annex 3

Work Stream 1 Supporting Analysis

Furthermore, in the analysis of a number of the critical tasks, recovery mechanisms are cited.

94 The use of NUREG 1792 to screen out actions does not seem appropriate methodologically (although it is noted that only one task was screened out in this manner). In the absence of a system-level analysis, the importance of issues such as post-maintenance checks, independent verification, valid checks during shifts, etc cannot be properly assessed. These are all actions that need to be included in a system-level analysis. Consideration of these actions also is needed both to confirm that the checks can be carried out and also to identify any design issues that might affect the ability to undertake the checks reliably.

95 4.1 - The exclusion of such tasks as planning, isolations and de-isolations is considered to weaken the value of the analysis and emphasises the importance of a system-level analysis.

96 4.3.2 - The elements of task support noted here as potential PSF do not facilitate consideration of concurrent tasks (e.g. other distracting or competing tasks that may be carried out during the maintenance period).

97 4.4 - It is noted that some of the task steps comprise inspection. It is not clear what consideration has been given to the design of the equipment, tasks or environment to facilitate reliable inspection.

98 4.4.1 - The requirement for Personal Protective Equipment (PPE) is noted, but it is unclear what this comprises. If it is full PPE then there will be implications for vision and communication associated with the use of respirators. See also 4.5.1. The additional comments in 5.3.6 are noted.

99 The assumption that the task is designed as a two-person task for peer checking purposes needs to be captured in order to ensure that the design does properly accommodate this.

100 4.4.2 - The role of post-maintenance re-qualification as a recovery mechanism is noted. This makes such activities important.

101 4.5 - The inability of the pump to achieve the required pressure is noted as a potential consequence. It is unclear whether this was reflected in the workshops as a credible failure mode, or whether those workshops considered only inability to run or complete failure of the pump.

102 5.1 - Violations might be better considered in the context of PSF, given the manner in which they have been addressed. In the absence of a system-level analysis, it is not clear that using violations only as a guideword in the workshop will allow a proper consideration of the design and the interactions between equipment design, task design and concurrent demands.

103 5.3.2 - Although the absence of training arrangements is noted and training is a post-GDA activity, there remains a need to consider the task design in terms of the demands it places on training. In particular, for the tasks under consideration here, they are infrequent and hence the training implication can become significant (infrequent tasks should not place great reliance on training and task familiarity).

Annex 3

Work Stream 1 Supporting Analysis

104 5.3.5 - The absence of a formal ergonomics assessment is noted. Some form of ergonomic assessment is possible, given the availability of the 3D model and design specifications for the environment. Any assumptions should be recorded.

105 5.4 - This section considers error recovery mechanisms. The absence of a systems-level analysis has already been noted. The importance of such recovery mechanisms raises concerns about the apparent manner in which such mechanisms have been screened out as being non-critical during the workshop.

106 5.4.14 - The reference to condition-based maintenance is significant. This is a fundamental change from previous practice. The significance of condition-based maintenance in terms of the demands placed on the inspection elements of maintainer actions is not clearly drawn out. The implications for the design of maintenance tasks may also be significant.

107 6.0 - The shortcoming in the TA Report Pro-forma should be explained.

108 The use of the workshop solely to identify critical tasks and hence the decision to terminate consideration of a task as soon as it has been deemed critical, has been commented on above. Is not considered a good use of the resources gathered together for the workshop, as this provides an opportunity to identify error modes and opportunities not previously considered and would provide a valuable input to the subsequent task analyses.

109 7.0 - There is no discussion in the Conclusions concerning the implications of the outcome of this analysis for the PSA. It does not consider whether any identified errors or error mechanisms affect the assumptions within the PSA.

110 Appendix C - As noted above, the rationale for rejecting recovery mechanisms as not being critical tasks is not considered clear. If the recovery mechanisms represented the final opportunity to correct a latent error then it may be a critical task. Important recovery mechanisms do not appear to be carried through to detailed task analysis, even though recovery mechanisms are cited in the detailed analysis presented in Appendix D.

111 Appendix D - The referencing system used is not helpful. Tasks appear to be given one set of references in the workshop (Appendix C) and then a different reference in the Task Analysis (Appendix D) which makes it difficult to cross refer.

112 General Comments:

- The method does not clearly show how a robust HEI process is applied.
- The conclusions do not consider how the outputs from the process can be used to support PSA and further design.
- There should be greater focus on the identification of errors, rather than the detailed analysis of tasks at an equipment level.

Example 4: Post-Fault Action (EFWS Refill)

113 This task was selected by EDF and AREVA for detailed analysis as it scored highly both for FV and RIF (both within the top 20 *HFEs*). The task is OP_FEED_TK, which requires the operator to cross-connect the Steam Generator (SG) tank and then re-feed the Start-

Annex 3

Work Stream 1 Supporting Analysis

up and Shutdown Feedwater System (SSS), MFWS or EFWS tank. The HEP identified for this task is $1.0\text{x}10^{-4}$.

114 My comments fall into two sets, being those that relate to how the example illustrates the generic method and those that relate to the specific Task. The first set concerns the Methodology.

Methodology Assessment

115 I consider that it would have been helpful to have stepped back from the specific analysis and considered the generic implications of their findings. For example, I consider that the findings imply that the PICS and operating philosophy is not optimised for supporting long-term monitoring tasks. I cannot determine what this means for other claims. I consider that the shortfalls in the PICS in this respect may be significant.

116 I do not consider the disregard of concurrent tasks and of dependencies to be appropriate.

117 I do not consider that the TA has provided due consideration of the SAP requirements and ALARP in respect of allocation of function (automation, etc.)

118 I consider that this TA highlights the need for a significant body of further work concerning both detailed design of the MCR and its formats/dialogues and, in respect of procedures, to ensure that the HMI and procedures adequately support critical monitoring activities related to successful execution of key claimed actions. It is unclear to me whether the claimed ability to monitor systems will be achieved. Additionally, it is important that issues arising from specific TAs, in respect of HMI and Procedures, are properly considered in a broader context.

119 A brief consideration of violations is provided, noting that issues outside the scope of GDA influence violations. However, the analysis does recognise that the nature of the task, involving long-duration monitoring, is likely to encourage pre-emptive actions (which could be considered violations). I consider that further discussion of how this tendency could be managed through design of the system should be provided.

120 This TA suggests that some of the actions noted in the HRA Notebook may be ambiguous and hence the claims associated with them may be unclear. The forward work programme needs to include review of the claims.

121 The value of running simulator trials when appropriate is made explicit, such as highlighting opportunities for enhancing PICS formats.

122 The OEF review appears to be based on a search for reports relating to feed-water alignments, etc. It is unclear whether a search was also undertaken for reports relating to long-term monitoring and similar tasks and whether this would have added value.

123 *Task Analysis Assessment*

124 I consider that this TA has omitted consideration of some key elements for this claim:

- Impact and relevance of the *“preferred source of make-up water via the demineralised water supply”.*

Annex 3

Work Stream 1 Supporting Analysis

- Potential impact of the initiating event, which is an unspecified external hazard. This could cause problems of access for LTP actions; cause considerable distraction for plant staff, etc. This is noted, e.g. in Limitations, but not taken into account.

125 This assessment has not considered 'acceptability' against ND SAP requirements:

- EHF.2 "*When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human action to maintain a safe state should be minimised*". Consequently, the assessment should have considered ALARP and partial/complete automation of some of the LTP actions encompassed by this claim.

126 Report conclusions – would be far preferable to conclude that the 10-4 claim is NOT supported unless the following points are adequately addressed.

127 The report notes the requirement for long periods of monitoring, but does not draw clear conclusions concerning the support to long-term monitoring provided by PICS and an operating philosophy that does not make use of alarms once AD has actuated.

128 It is noted that the defined scenario is with all four trains available, as scenarios with fewer trains available are lower risk. However, it is also noted that scenarios with fewer trains may be more demanding for the operators. This raises questions concerning the reliance on risk-based screening for selection of tasks for detailed analysis.

129 Dependencies have been explicitly excluded from the analysis. Proper treatment of dependency requires explicit modelling (as noted in HRA TAG). Such modelling needs to be informed by task analysis and hence it would seem helpful for these TAs to provide some discussion of potential coupling mechanisms, even if they do not attempt to quantify the effect of such dependencies.

130 Some potential errors are noted, such as navigation errors, which could lead to incorrect diagnosis or plant status identification. No analysis of the potential consequences or their significance is provided. Some form of 'confusion' analysis would seem appropriate for navigation and use of PICS-style interfaces.

131 This claim is highly reliant on MCR monitoring of EFWS status and inventory over a protracted period, without optimised information presentation to support that monitoring process (e.g. absence of trend information)

132 LTP actions are 'time constrained' by reliance on MIN3 level indication. The HMI appears to me to be inadequate for supporting monitoring of EFWS status.

133 The EDF and AREVA assessment has identified noted deficiencies with existing arrangements and made sensible recommendations for improvement. This highlights both the benefit of undertaking these task analyses and also the impact that their absence to date appears to have had on the adequacy of the design.

134 The potential impact of the 'preferred demineralised water supply' is not considered adequately:

- If there is a preferred source, there needs to be greater clarity of what that will mean in terms of procedure and task sequence, execution times, etc.

Annex 3

Work Stream 1 Supporting Analysis

- If no preferred source is modelled in the PSA there needs to be greater clarify of why the operator is given flexibility and how that flexibility s to be controlled (whether by procedures or by training).

135 The time requirements for LTP actions (and the need for actions in four separate zones) suggest automation should be considered for EFWS tank level control, but this does not appear to be considered within the TA.

136 If no automation is to be provided, then monitoring needs to be made far more robust. Timing and sequencing of actions needs further consideration (such as to allow for the use of a preferred water source) and partial automation of LTP actions should be considered (such as providing MCR controls for cross-connection and tank make up). The TA does not appear to consider these options and hence I have less confidence in the manner in which the TAs will be used to inform and improve design.

137 This example shows ‘tactical’ level diagnoses involved in implementing SOA strategies – and the importance of HMI and procedures in making correct diagnoses. I do not consider that the analysis gives sufficient attention to the manner in which such diagnoses can be disrupted.

138 No detailed discussion is provided concerning the operating philosophy that requires cycling through the procedure for loss of CCWS for up to 100 hours and whether the system provides adequate support for such a requirement, given the concurrent activities that are inevitable over such a period of time. Consideration of concurrent activities is explicitly excluded.

139 I am unclear what the basis is by which issues are selected for entry onto the HFIR. Not all issues seem to be captured by HFIRs, e.g:

- P.36 SME statement that cross-connection will be undertaken as a separate first action. This is an important point for the procedures as it indicates that the SME considers that the existing procedure is inaccurate. I assume that the issue has been captured elsewhere, but I would expect the HFIR to include a complete record of issues arising from the TAs.
- A recommendation has emerged from the analysis in respect of the MOP KAE 3118 YP. The recommendation is that it should call up detailed EFWS display screen 3ASG0002 YC. This does not appear to be captured within the HFIR.

140 A further issue with the HFIR is noted in HFIR 037, where the need for a compelling cue for EFWS tank criterion is noted and a recommendation is made for an acoustic alarm. I consider this recommendation inappropriate as it is in conflict with the declared operating philosophy that discards the response to alarms once SOA invoked.

Specific Issues Arising from the TA

141 For manual actions, I consider that there is a need to improve the HMI for EFWS status monitoring and to devise more robust procedural arrangements for monitoring (to ensure reliable early recognition for cross connection and make-up actions)

142 The conclusions appear to me to be focused primarily on the ease of performing both MCR and LTP actions, once the requirement has been identified. The shortcomings with respect to long-term monitoring from within the MCR are not emphasised. These may be

Annex 3

Work Stream 1 Supporting Analysis

generic to other long-term monitoring activities. An assessment of the generic implications with respect to the HMI within the MCR should be provided.

143 The impact of the preferred demineralised water supply and the nature of the IE need to be further considered

144 The issue of the effect of the IE and external hazards on the achievability of the required tasks is noted and the uncertainty that this introduces for estimating task time durations. Uncertainty is also noted concerning the time taken to determine the required make-up source. This raises doubts concerning conclusions with respect to time availability and time pressure.

145 It is noted that certain PICS formats present key information for monitoring tasks, but that the use of these formats may not be specified within the procedure. The linkages between procedures and formats therefore may need to be reviewed, given the absence of reliance on alarms to support monitoring.

146 The analysis considers that time pressure is minimal, because the 100 hour inventory is not explicitly communicated to the operator by the HMI or the procedures. However, it is reasonable to expect SQEP operators to be aware of this and the absence of indications on the HMI could actually increase perceived time pressure by introducing unnecessary uncertainty. This should be considered further.

147 The absence of a procedural requirement to monitor the tank as it is being filled and hence to stop filling at an appropriate time, is noted. It is not clear what the potential recovery mechanisms are (the analysis indicates who could recover, but not what information is available to support recovery).

148 The allocation of function conclusion appears to be based on the assessment that the task is simple. Whilst the LTP actions may be simple, the operator actions within the MCR appear to have some complexity, and hence the AoF decisions with respect to MCR activities may not be correct.

Annex 4

Work Stream 2 Supporting Analysis

Introduction

1 Work Stream 1 aims to assess in detail the substantiation of the HRA and to a certain extent Work Streams 3 and 5 also support the assessment of the HRA substantiation. Work Stream 2 aims to look generically at particular aspects of the HRA across the safety submission, particularly relating to HRA methods and application. The material presented in this annex is provided as supporting analysis to the information presented in the main body of this report. It relates mainly to data derivation, to support my judgements on the applicability of extant HRA methods and the EDF and AREVA approach to the HRA, as discussed fully in the main body of the report.

Relevance of Extant Human Reliability Assessment Techniques for the Assessment of Modern Control Room Task Environments

2 In this section I present details of the experimental studies that informed my judgement on the relevance of the HEP data points in THERP to contemporary control room environments.

3 In principle, it could be argued that the levels of reliability likely to be obtained in a particular interaction between a human and a computer are likely to be similar to those obtained when interacting with discrete controls and displays. For example, whilst the method of interaction and selection is different, it might be argued that selecting one navigational target from a number of navigational targets on a screen requires the same psychological mechanisms of recognition and discrimination that are required for selecting the correct discrete control or discrete display on a panel. However, in the absence of data this is supposition.

4 Claims for human reliability are an integral part of the PSA. Therefore, any potential optimism in the assessed levels of human reliability may imply a higher level of safety than is like to be the case in accident conditions.

5 Accordingly, this work aimed to assess whether there are substantial differences between available HCI data regarding human error and the reliabilities suggested by THERP. In this context a substantial difference would be one that could be significant for risk assessment. For current purposes, I consider this to be half an order of magnitude or greater.

6 The literature obtained can be split into that offering information relating to holistic tasks and that relating to more discrete or object level tasks and this is how I have reported my findings.

<u>Experimental Studies – Holistic Tasks</u>

7 A holistic task is one where the task has either been performed within its real world context, or simulated at a level of fidelity where the essential real world features that could affect HCI error, have been replicated.

8 Four studies were identified where tasks and human error were studied and measured at the holistic level.

1 A Taiwanese study (Ref. 22) examined nuclear power plant start-up performance of teams working with automated support for their procedures and interface. All

subjects were drawn from a nuclear engineering institute. Half the teams comprised nuclear engineering students whilst half were operators or experts. Therefore, the reported level of error in the study may be higher than that which would be expected in practice. Errors were reported at the level of interaction task failure commensurate with THERP.

2 A study of the performance of a collaborative virtual team distributed across global office sites examined the error rate per task (Ref. 23). Within this study, observations were obtained from day-to-day work and therefore tasks and errors could be of any kind. Errors were measured at an hourly rate. To derive an estimate of error probability and based upon information given within the paper, it has been assumed that one task is performed every two hours. (It should be noted that, if it is assumed tasks performed more frequently than the estimated error probability, will go down. It seems unlikely that a task would be performed less frequently). This study would be relevant to interactions and support by remote teams such as remote Emergency Support Centres.

3 An experimental study examined decisions about the acceptability, or otherwise, of parametric (i.e. numerical) process data presented in tabulated layouts, very similar to alarm listings. The study examined three experimental conditions (Ref. 24). Significant experimental differences obtained in the study were of no practical significance in terms of error. Nevertheless, the marginally most conservative estimate of human reliability has been taken from this study.

4 A study investigated the level of knowledge and understanding of automated processes as a function of training, experience in use and attentional focus when used (Ref.25). Attentional focus was the level of attention given by the users to the automated system when it operated. This was found to be a function of its perceived importance to system users and the extent to which it interacted with their manually controlled task and made its impact known upon the wider system state.

<u>Experimental Studies – Object Level Tasks</u>

9 Object level tasks are those more traditionally associated with experimental psychology and concern particular elements of human-system interaction, such as item selection. As such, they are often undertaken in experiments without a particular context and are abstract in nature.

10 The studies of human interactions at the object level produce broadly similar results and therefore, studies are not described separately but in overall groupings. However, the significance of the studies can be considered as a whole.

Vision, Parallax and Foreshortening

11 An experimental study (Ref. 90) sought to establish the extent to which process control information images can be foreshortened before errors occur. Normal to the line of sight errors were reported 2.0×10^{-2} whilst a process display, foreshortened to be at 45° relative line of sight, had errors reported at 2.0×10^{-1}. For practical purposes, the error rate can be supposed to increase linearly between these two values for different angles between these limits. This has practical implications for the reading of shared displays such as

plant overview displays. No comparable data exist pertinent to this issue in any of the HRA methods and the extreme unreliability which is shown, demonstrates that it is an issue which must be categorically eliminated by deterministic design.

Interactions with Icons and Labels

12 A study has shown over an order of magnitude increase in reliability by double clicking rather than single clicking an icon in order to select it. Nevertheless, the best error rate obtained is still only 5.0x10^{-2} (Ref. 91). This is over two orders of magnitude less reliable than the reliabilities for selection that might be suggested when examining the THERP tables for the selection of controls and displays.

13 Two separate studies examining the influence of icons, with or without labels or help, (Ref. 92) and a study of labels (Ref. 93) lead to the conclusion that icons with labels are no more reliable than labels alone, but labels should be adjacent to the item annotated and that their reliability in use is of the order of 5.0x10^{-2}. Again, labels are central to the process of selection and this is over two orders of magnitude less reliable than selection performances suggested by THERP.

Interactions with Menus

14 Three studies have examined human performance and error as a function of design features in menus (Refs 94, 95 and 96). These do not clearly establish if menus should be designed so that each successive menu replaces the last. However, they do make clear that menus should emphasise items that are frequently used, possibly eliminating unused options, but the order and spacing of presentation should never change. The last study (Ref. 96) also establishes that the overall hierarchical structure of menus should be shallow and wide.

15 These features, when taken together with left justified text, might be expected to lead to a best error probability of 7.0x10^{-3} when interacting with menus. This statement assumes that the reliabilities in the individual studies can be additively combined. In practice, this may not be so and the estimated reliability may not be as good as that estimated. It is very important to note that reliabilities, when reported in individual studies, are approximately an order of magnitude less reliable at about 4.0x10^{-2} to 6.0x10^{-2}. If it were to be suggested that THERP selection reliabilities would be appropriate for HCI menu item selection, then estimates would be over two orders of magnitude more reliable than appears to be appropriate based upon reported data.

Interactions with a Mouse

16 Two studies, (Refs 97 and 98) examined interactions using a mouse and found reliabilities for the tasks in question to be between 4.0x10^{-2} and 9.0x10^{-2}. It is important to note that one task was a simple graphical editing task whilst the other had a complex psychological dimension. In the complex psychological task, the user was required to select, for example, the word "red" but displayed in a yellow font. This is known as the Stroop experiment. An important effect was found in this study whereby mouse interactions were much slower than the alternative means of selection using a keyboard but much less prone to error. Measured human reliability flatly contradicted subjective preferences for the keyboard. Keyboard error rates were a factor of three worse at approximately 1.0x10^{-1}.

Annex 4

Work Stream 2 Supporting Analysis

Interactions with Soft Keyboard

17 A number of studies of keyboard use are reported in the literature, but these do not alter existing understanding of keyboard reliability for a tactile keyboard. The highest reliability for tactile keyboard key striking per key is reported at 3.0×10^{-3} (Ref. 99). This contrasts with the best reported reliability for a soft on-screen keyboard of 6.0×10^{-3} per key (Ref. 100). This latter experiment arrives at a counterintuitive conclusion that a soft keyboard is most reliable when the keys appear on screen in random positions. However, this is for a non-time constrained task using novice users. However, they have been trained in keyboard use and I consider it debatable whether further experience would produce any significant improvement in the levels of performance and error reported in the paper reviewed here. It is noteworthy that a large soft keyboard with consistent positions has an entry error rate of 2.5×10^{-2} which is exactly 10 times greater than that for a tactile keyboard. This study strongly suggests that on-screen keyboards should never be used where reliable data entry is required. There is no comparable entry within THERP for keyboard entry. An on-screen keyboard is half as reliable as the baseline probability for SPAR-H and the SPAR-H baseline probability of 3.0×10^{-3} for a keyboard command would probably be optimistic if the analyst undertook the assessment at the ‘keyboard phrase’ level not the keystroke level. Of course, in practice, this would be entirely dependent upon the level of feedback available and sought by task performers about phrase entry. I therefore conclude that THERP has no appropriate data for keyboard entry and application of SPAR-H would also provide an optimistic assessment.

Data Entry

18 One study (Ref. 101) examined the number of digits that could be entered reliably from working memory. This confirms classical psychological experiments on the ‘Span of Apprehension’ and suggests that the one to three digits, reliability is 5.0×10^{-2} whereas for eight to10 digits reliability is an order of magnitude less. This compares unfavourably with THERP table 20 – 10 which suggests a negligible error probability of three digits and 1.0×10^{-3} per digit for more than three. For HCI data entry, I conclude that THERP appears to be optimistic by at least an order of magnitude.

19 Another interesting study (Ref. 102) examined code line errors for the configuration of a railway interlock system. In this study, a distinction was made between errors of knowledge and skill or rule-based writing errors following Rasmussen's taxonomy. Writing errors were found to be at 9.0×10^{-2} per line whereas errors of knowledge were found to be at 3.0×10^{-3} per line. This is unusual, because the cognitive/knowledge error rate is lower than the skill or rule error rate.

20 It can be concluded that HCI data entry errors are firmly in the region of 5.0×10^{-2} to 6.0×10^{-2} and dominate interlock programming errors typified at 3.0×10^{-3}. (It should be noted that the programmers of railway interlocks do this job all day every day and are very familiar with the simple methods for interlock rule declaration. Therefore, it can be argued that the reliability obtained in the study reported is probably towards the lower end of what can be achieved across the gamut of safety system programming tasks. Nuclear interlock programming may be more variable and therefore less reliable.)

21 For SPAR-H and ASEP, it seems unlikely that the analyst would apply unreliability on a per-line basis as reported in the literature. Even if applied on that basis, results could be optimistic.

Annex 4

Work Stream 2 Supporting Analysis

Procedure Following and Decision Making

22 Three studies are reported within which procedure following and decision making are undertaken. It is important to note that not all the tasks were process control but involved aircraft readiness (Ref. 103), decision-making about the first aid treatment of personnel following chemical release (Ref. 104) and the fault diagnosis of a chemical process plant involving feedstock mixing heat exchanging product and waste storage (Ref. 105). In all three studies, the subjects had sufficient technical expertise to deal with the task content in principle but had no previous experience of performing tasks in practice. However, training in system use was provided in all cases. Nevertheless, human error ranged from $1.0x10^{-1}$ to $5.0x10^{-1}$ in the best experimental conditions encountered within each study. These studies clearly demonstrate that, even with automated HCI-based task support, cognitively intensive tasks decision making tasks can be unreliable. Within the studies in question, experimental factorial differences did not exceed four. Therefore, it would be reasonable to infer that performance might improve at most by a factor of four, i.e. over a range of $3.0x10^{-2}$ to $1.0x10^{-2}$ with greater experience in system use. These reliabilities are considerably less than some that are proposed by THERP in Tables 20-21 and 20-23. ASEP uses the same tables and the same conclusion applies.

23 SPAR-H is derived from THERP but it is unclear whether the proposed reliability for diagnosis is intended to be for an individual or team. If it is taken by an analyst to be for an individual, then the SPAR-H baseline reliability of $1.0x10^{-2}$ would be made optimistic if the decision support offered by HCI is considered an asset and used to improve the baseline probability. If, however, the baseline of $1.0x10^{-2}$ is interpreted to be team reliability (as should probably be the case) then it might be a potentially conservative estimate. However, this would be entirely dependent upon the potential for recovery of error by others.

Interface Language

24 Two studies have examined the effects of consistent and inconsistent interface terminology and an interface having a mixture of a local and foreign language within it. Unfortunately, the study examining terminology (Ref. 106) does not report error rates but measures an experimental difference of four between consistent and inconsistent use of terminology. However, the study involving the use of mixed languages in the interface (Ref. 107) does measure error rates within which an experimental difference of two is found between the use of a consistent and inconsistent use of local language at the user interface. However, in interpreting the findings of the latter study, it should be noted that the foreign language was English and all users had this as a regular second working language. Overall, it is concluded that a simple interface with consistent use of language will produce error rates of around $3.0x10^{-2}$ in interpretation, which approximately doubles with the second working language used. However, if the language is mixed the error rate increases by a factor of five to $1.5x10^{-1}$.

25 The studies show the potential importance of language on the interaction performance of an HCI. Neither THERP, ASEP nor SPAR-H recognise this potential source of error.

Secure Log on

26 An interesting study is reported within which the users of a public website had their performance monitored in logging on securely over a long period (Ref. 108). This study

is reported here, not for any insights it might give about interactions to secure log in on, but for insights it gives about measures of performance with and without the opportunity for error recovery. The website in question had been specifically designed to be accessible to all the people. Accordingly, login consisted of them recognizing a sample of their own handwriting which displays their logon number. The reported error rate for logon without recovery was 2.0x10^{-2} and with recovery this improved to 1.0x10^{-2} at the second or third attempt. However, there was an additional likelihood of 1.0x10^{-2} that the logon attempt would be abandoned entirely. This shows that where an HCI offers choice, recovery rates can be low.

Possible Pessimism in Experimental Studies

27 In providing judgement on the suitability of extant HRA techniques (e.g. THERP) for tasks involving advanced interfaces it is necessary to consider the artificiality of the experimental data discussed in the preceding sections. By their nature, such experiments will seek to identify all errors regardless of any subsequent recovery or consequences. It could be argued that unsuccessful interactions with menus, inappropriate ‘mousing’, breakdowns of keyboard entry and icon selection are all amenable to self recovery. In fact, ‘error tolerance’ is a sought after characteristic of such interfaces. This raises the prospect that experimental studies, which measure error without feedback of the error and opportunity of recovery, are pessimistic.

28 There are a number of perspectives to this issue. Firstly, interactions with computers that will have a functional result in risk terms, e.g. the operation of the control or the monitoring of a display to observe a safety-critical parameter will contain within them a number of elemental object interactions. If any of these elemental interactions possess a probability of error that is perceived by the task performer, this raises the level of distraction and may reduce attentional focus on the process plant, so making functional errors more likely.

29 Secondly, if one recognises that some interactions with objects, such as menus and icons, have the potential to have a direct functional result with consequences upon the process, then the likelihood of self recovery must be explored. Attention has already been drawn to the recovery in security logins where the resulting error rate was effectively halved (Ref. 108). However, users were not compelled to continue the task and could simply cease their interactions. As a result, this may not be a good representation of recovery. A comprehensive study on the use of icons provides better indication. When uncertain about an icon, users were able to consult online help (Ref. 8). It is reasonable to argue that consulting help constitutes evidence of a subject anticipating a breakdown in their knowledge required to complete the task successfully. In effect, this is pre-emptive error recovery and is an overt manifestation of self checking and error correction behaviour.

30 Artificially assuming that each consultation of help pre-empted an error, examination of the data given within the paper shows that, for every error made, about eight were prevented by consulting help at the highest error rates (9.0x10^{-2}) and at the lowest error rates (4.0x10^{-2}) there were 23 consultations of help for each error made. For an approximate halving of the error rate, help consultation went up by a factor of nearly three. It is also significant that the online help is consulted approximately two and a half times more often when a label is present either alone or with an icon than when the icon

Annex 4

Work Stream 2 Supporting Analysis

is presented alone and yet an icon alone is the least reliable interface. This suggests that the least informational redundancy leads to the least consultation of online help, or possibly that the presence of a label allows a user to better detect if there is ambiguity at the user interface and their understanding of it.

31 Another cited study (Ref. 98) has also amply shown that the preferred solution was chosen by subjects because it could be used most quickly, but it was also the most error prone *per user interaction.* These last two studies reveal an important general HF conclusion that, whilst people may be good in assessing their throughput performance, they are bad at assessing their performance in terms of the numbers of errors made, particularly where the influence of potential time saving is apparent.

Sensitivity to Performance Shaping Factors

32 It is not unusual for HF experimental studies to identify statistically significant differences between aspects manipulated by experimental conditions that are of little significance in terms of human reliability, particularly when considered at a holistic task level. Such a difference would be less than a factor of three, which is commonly regarded as the minimum reasonable achievable accuracy in HRA due to factors such as the effect of training in masking smaller effects. As part of this work, the magnitude of experimental effects has also been examined. Any descriptions of experimental effects that follow in Table A4.1 are expressed as the simple arithmetic mean effect.

Table A4.1: Reported Experimental Effects

Good condition-versus-poor experimental condition	Effects => 3
Visual line of sight: straight on versus 45° parallax.	13
Icon selection double-click versus single click.	4
Icon with label and help versus unhelped, unlabelled icon.	8
Menu item selection with used items highlighted versus unemphasised menu.	3
Presentation of the next level of menu hierarchy versus no presentation of the next level.	3.5
Drag a graphical modifying function to a shape versus drag an shape to a modifier.	3
Select objects reliably with a mouse versus with keyboard.	3
Input using a tactile versus non-tactile keyboard.	10
Data entry chunked in two’s string length up to three digits versus up to 10 digits.	12
Database searching by elderly (i.e. over 60) versus young people.	5
Automation knowledge with frequent exposure and good attentional focus versus infrequent exposure and weak attentional focus.	10
Practised diagnoses with automated support versus unpractised.	3

Annex 4

Work Stream 2 Supporting Analysis

Table A4.1: Reported Experimental Effects

Good condition-versus-poor experimental condition	Effects => 3
Inconsistent use of terminology and meaning at the user interface versus consistent.	4
Number of performance shaping factors in 20 cited studies with effects greater than 3	13
Average experimental effect	6.75
Maximum effect	13

33 Significant experimental effects seen in the cited studies, as shown in Table A4.1, generally produce results which are also significant in risk assessment terms. This is a matter for concern because, unlike interfaces comprised of discrete controls and displays, the same degree of design codification does not exist on what constitutes an HCI, which can produce good human reliability. Technological development also impacts this issue as it provides further and further means by which users can interact with systems (e.g. the advancement in touchscreen technology for consumer products in recent years).

34 In a recent survey amongst HCI designers concerning a draft standard for interface design (Ref. 109), it was established that approximately half the usability issues encountered by respondents were unique and unlikely to be addressed by such a standard. This statistic must, to an extent, be a function of the relative inexperience in the design and HF community on the one hand and the wide degrees of freedom within computer software and operating systems to design novel means of interaction, on the other.

35 The OECD Halden Project has considerably greater experience than most in understanding what factors will lead to good and poor human performance at the user interface. In formulating the complex scenario for the International Empirical HRA Study they simulated two of three SGs with faulted wide-range level instruments (Ref. 110). The scenario involved a requirement for Bleed and Feed and the initiation criterion for this was that two of three SG levels should be below 12% wide-range. Of ten trial crews, three crews suspected failing SG level measurements. This was despite the fact that two of three indications were faulted and one was giving a true indication. Notwithstanding this situation, although indication of conditions was given a main negative driver, the HMI was rated as a nominal or positive performance shaping factor. However, the user interface was clearly deficient because questionable data indications would have provided much clearer indications that level indications were faulted. As it was, only one crew in ten actually started the bleed and feed on low SG level giving a nine out of ten ($9.0x10^{-1}$) failure rate of meeting the primary initiation criterion. This shows that, despite their extensive expertise at the OECD Halden Project, interface assessors and designers can fail to correctly recognise the significance of user interface features (or their absence) upon human performance.

Annex 4

Work Stream 2 Supporting Analysis

36 The Halden study also invites the counterfactual argument that, the presence of doubtful or questionable data validity indications would have probably produced a step change improvement in the diagnostic/decision making performance exhibited by the trial crews.

Error recovery and supervision

37 No studies were identified which examined the rate of error recovery as a result of direct supervision or a second person monitoring the same process information. However, one study (Ref. 102) was identified which investigated recovery of railway interlock programming errors by means of code checking (i.e. reading the code) and testing (i.e. running the code).

38 The examination was of the actual error logs from a number of different signalling companies and projects. However, a lack of consistency between the methods of login and the inability to know what had been entirely missed, meant that estimation of statistics for the recovery were not possible. An experiment was, therefore, undertaken within which actual faults were taken and subjected to checking and testing processes by novices. For checking, the probability of failing to detect a fault ranged from $3.0\text{x}10^{-1}$ to $1.0\text{x}10^{-1}$. The testing ranged from a zero error rate to $6.0\text{x}10^{-1}$. Of course, the reliability of testing is as much a function of the capabilities of the testing methods as it is of human performance.

39 This same study also identified a false alarm rate (i.e. the identification of non-existent faults) of around 25% overall. It is reasonable to speculate that over the long term, such a high false alarm rate might be expected to lead to a reduction in the effectiveness of checking. Indeed, it is interesting to note the qualitative findings of the study. They found it possible to categorise faults as either skill/rule-based or knowledge-based. The investigations of the error logs from signalling projects showed a far higher incidence of knowledge-based errors being detected than skill/rule-based errors. This was also reflected in interviews with programmers who placed considerable importance on detecting knowledge-based errors and, it seems, expressed an implicit belief that these were more likely. As previously stated, the knowledge errors are less likely when recorded per line of code, but this does not reflect the frequency with which knowledge is demanded. However, when they occur, knowledge errors tend to have a wider propagating effect within the resultant code.

40 Whilst the information on error recovery may be of interest for HCI system development, it is probably of little relevance to the control room experience where post fault tasks are paced by transient timescales.

Generic Human Reliability Assessment

Data-Based Estimates of Diagnostic Unreliability

41 In this section I derive estimates of cognitive or diagnostic unreliability within fault scenarios based upon data available within published literature.

42 In the 1980's Beare *et al.* (Ref. 111) found that the unreliability in performance of tasks involving nuclear plant realignment following procedures in normal circumstances was of the order of $3.0\text{x}10^{-3}$. Sheue-Ling Hwang *et al*. (Ref. 22) for a computerised procedures supported NPP startup and checking by dedicated supervisors with no other tasks and

with no perturbations, estimated unreliability at 2.0x10^{-3}. Beare and Sheue Ling Hwan, taken together, might suggest that the limitation on NPP crews' performance in normal circumstances is not bounded by the degree of task support offered to them but by a ceiling in possible crew performance. As these studies measured crew performance in normal unperturbed circumstances, it is reasonable to suppose that they might represent a bound on the level of cognitive crew performance that is possible. Self-evidently, it should be better than in situations where there are perturbations with the attendant added stress and the potential for unexpected evolutions in plant transients.

43 Hannaman, Spurgin, and Lukic (Ref. 35) in their simulator, based studies of the probability of crews responding to a fault by a given time generated curves for post fault operation. These show no probability better than 1.0x10^{-3} for knowledge-based performance and their geometric mean probability for their distribution of performance is 3.0x10^{-2}. However, it must be borne in mind that in deriving their non–response probability curves, there were outliers in their data and some tested crews did not respond appropriately at all on any timescale. These data were excluded, giving crew non-response probability estimates of 2/14 crews or 2/16 crews (i.e. 1.0x10^{-1} or 6.0x10^{-2}) according to the particular study. In other words, their response curves show the probability of a crew response in a given time, given that they successfully recognise/make the correct diagnosis of the circumstances.

44 I have not found data to suggest that cognitive performance can reach the human performance limiting value of 1.0x10^{-5} as suggested in the THERP Table 20-3. This level of reliability seems to be most unlikely to be the case in all but the most trivial of faults. Dougherty and Collins (Ref. 112) reported that highly reliable skilled manual performance at around 1.0x10^{-5} can be achieved for very carefully executed often-repeated missile maintenance tasks performed by a highly skilled single individual. As described by them, the tasks are not ones characterised as requiring high levels of knowledge-based cognitive performance. It therefore seems unlikely that the rare event cognitive diagnosis of a nuclear power plant fault is likely to meet the conventionally declared HPLV.

45 All of the foregoing data describes the bounds of cognitive knowledge based performance. There are other data available which describes performance within simulator based post fault scenarios. It is reasonable to assume that emergent error rates will be dominated by cognitive error rather than inherently more reliable skill-based performance.

46 In the performance of two cognitively demanding simulated emergencies by Roth *et al*. (Ref. 85) of the Westinghouse Electric Company Science and Technology Center, it was found that approximately 1.0x10^{-1} of crews did not have correct situation assessment for one loss of heat sink scenario. The study examined crew performance in variants of an Interfacing System LOCA and a Loss of Heat Sink scenario. This study also demonstrated that operators do not follow procedures by rote, but actively participate in diagnostic activities and exhibit cognitive performance during fault identification. Although not its primary purpose, this study suggests an emergent error rate which corresponds to that put forward by Williams in the Human Error Assessment and Reduction Technique (HEART) method (Ref. 113) who suggests that tasks described as *"Complex task requiring a high level of comprehension and skill"* have a nominal error probability of 1.6x10^{-1} for a single individual. Williams for his task, places uncertainty bounds on this task of 2.8x10^{-1} to1.2x10^{-1}.

Annex 4

Work Stream 2 Supporting Analysis

47 Extensive simulator studies of post-fault crew performance have been recently undertaken at the OECD Halden project as part of the international empirical HRA study to test the effectiveness of HRA methods. The results of crew performance are published in Broberg *et al*. (Ref. 110) and Bye *et al*. (Ref. 114). These respectively report on variations of Loss of Feed Water (LOFW) and SGTR scenarios.

48 The Halden scenarios ranged in complexity from four coincident faults to routine post-trip actions. The most complex scenario involved an SGTR with coincident steam line break, electrical bus failure and a leaking/passing Pressure Operated Relief Valve (PORV). The simplest or based scenario involved stopping all but one charging pump and closing the two Boron Injection Tank inlet and the two outlet isolation valves. Other scenarios are diminishing degrees of ranked difficulty from the most complex by virtue of having less coincident faults. Of these, six involved SGTRs and two involved LOFW. The types of faults were not confined to process plant faults but also included instrumentation faults such as SG levels giving false readings and a complete absence of radiation indications.

49 The measured and reported error rates from the studies outlined above that included simulated faults are tabulated in Table A4.2 below.

Table A4.2: Diagnostic Human Error Probabilities from Literature

Reference	Crew HEP
Hannaman *et al.* (1985) geometric mean.	$3.16\text{x}10^{-2}$
Roth *et al.* (1996).	$1.0\text{x}10^{-1}$
Broberg *et al.* (2009).	$2.0\text{x}10^{-1}$
Broberg *et al.* (2009).	$9.0\text{x}10^{-1}$
Halden (2009) 5B1.	1
Halden (2009) 3B.	$2.14\text{x}10^{-1}$
Halden (2009) 3A.	$1.43\text{x}10^{-1}$
Halden (2009) 1A.	$1.43\text{x}10^{-1}$
Halden (2009) 2A.	$1.43\text{x}10^{-1}$
Halden (2009) 2B.	0 / unknown
Halden (2009) 5B2.	0 / unknown
Halden (2009) 4A.	0 / unknown

50 In three of the Halden scenarios (Bye *et al*.) no crew errors were observed. For each of these three scenarios, 15 crews performed the exercise. Therefore, the actual HEP for crew performance in these scenarios remains unknown. In order to estimate the possible range of probabilities, the study used a Bayesian approach. A minimally-informed prior

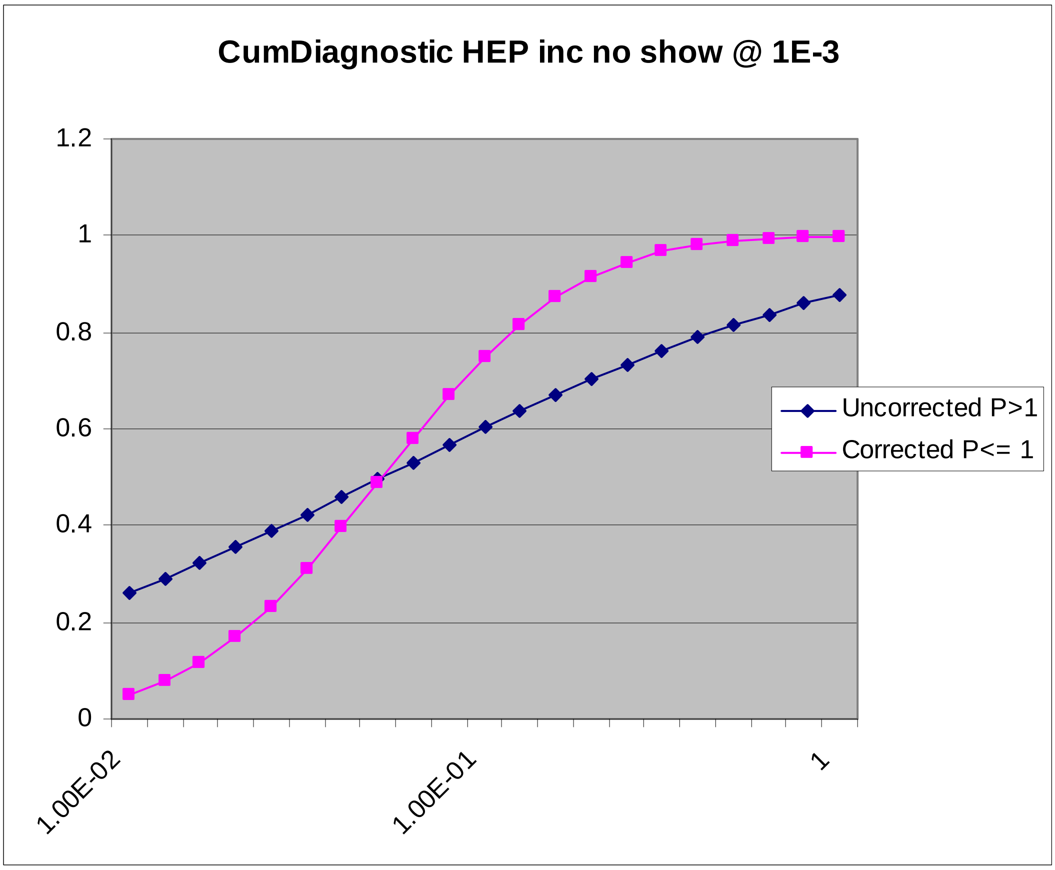
Annex 4

Work Stream 2 Supporting Analysis

distribution was defined, having a lognormal distribution with a fifth percentile of $1.2\text{x}10^{-4}$ and a 95th percentile of 0.3. These represent some of the lowest and highest values expected for HEPs of operator actions and correspond to an error factor of 50. However, based upon the survey of sparse evidence in literature shown above the fifth percentile of $1.2\text{x}10^{-4}$ would appear to be optimistic. Accordingly, the issue remains open on what estimate should be used for human error for the three scenarios for which no error or ‘no show’ was observed if an overall estimate of cognitive performance within fault scenarios is to be derived.

51 I consider that there are two plausible estimates for error that can be put forward for the missing data. The first is to assume that all three scenarios will represent crews performing at the best published and justified estimate for cognitive performance. This will be the $1.0\text{x}10^{-3}$ estimate of Hannaman *et a*l. (Ref. 35). An alternative estimate would be the central estimate from their work as this is the only published distribution for cognitive performance (be that knowledge-based or rule-based) available. The geometric mean of either distribution is $4.0\text{x}10^{-2}$. An alternative approach is to propose no limits for the missing data and to exclude these scenarios from further consideration. The results of using a best estimate, central estimate and excluding the three scenarios are shown in the three figures below.

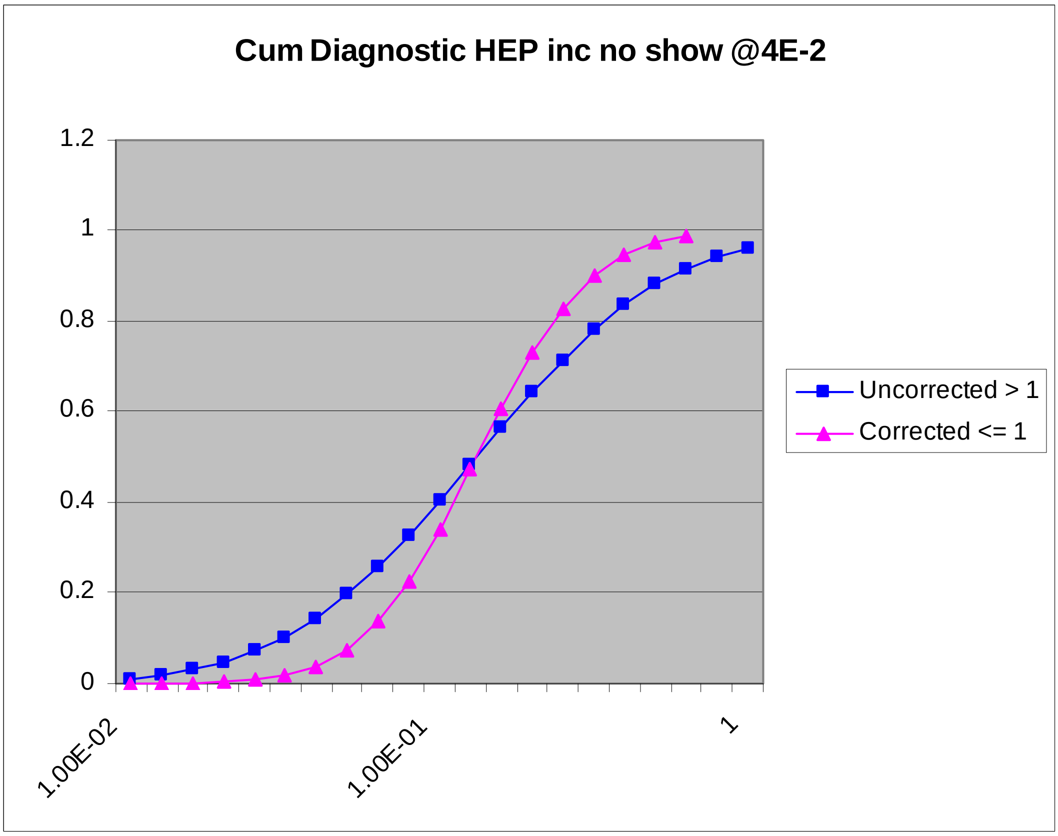
Figure A4.1: Cumulative Error Probability with Missing Data Estimated at $1.0\text{x}10^{-3}$



Annex 4

Work Stream 2 Supporting Analysis

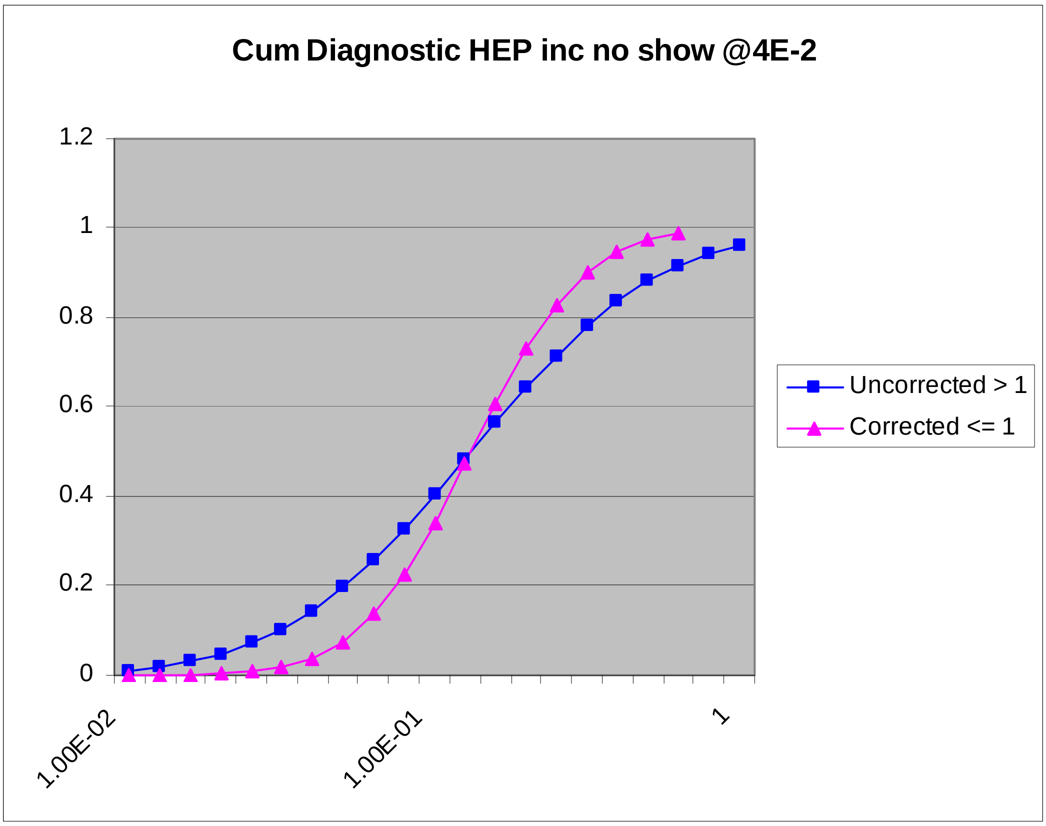
Figure A4.2: Cumulative Error Probability with Missing Data Estimated at 4.0x10^{-2}



Annex 4

Work Stream 2 Supporting Analysis

Figure A4.3: Cumulative error probability with missing data excluded



52 Each of the three distributions uncorrected logarithmic cumulative frequency curves reaches their asymptote at an estimated probability (shown on the x-axis) that exceeds one. These curves are blue. Clearly, this is an impossible outcome. Accordingly, a statistical adjustment has been made about the mean for each distribution. This is achieved by assuming that each distribution is symmetrical and that the maximum and minimum logarithmic value for each is situated three standard deviations either side of the mean logarithmic value. The adjusted distribution retains the same mean value but accordingly provides different estimates for the fifth and 95th percentile error probabilities for each of three given ranges.

53 Table A4.3 below summarises the resulting fifth, mean and 95th percentile estimates according to the chosen treatment for the scenarios within which no errors were observed.

Table A4.3: Summary of Distribution Limits and Means by Missing Data Estimate

Missing Data Estimate	5th centile	Mean	95th centile
Data excluded	$8.0x10^{-2}$	$2.0x10^{-1}$	$5.0x10^{-1}$

Annex 4

Work Stream 2 Supporting Analysis

Table A4.3: Summary of Distribution Limits and Means by Missing Data Estimate

Missing Data Estimate	5th centile	Mean	95th centile
$4.0x10^{-2}$	$2.0x10^{-2}$	$1.0x10^{-1}$	$4.0x10^{-1}$
$1.0x10^{-3}$	$1.0x10^{-2}$	$5.0x10^{-2}$	$3.0x10^{-1}$

54 Table A4.4 contains 12 data points. It is possible that substituting the same estimated error rate into all three *"no show scenarios"* could have an undue influence on the overall estimate of the mean and range for error. However, examination of the three rows of estimates, each with different substitutions, in Table 2 shows that this is not the case. It will be noted that the 95th percentile error probability estimates change little and a best estimate would appear to be $2.0x10^{-1}$ or $1.0x10^{-1}$. For the fifth percentile estimates, either $2.0x10^{-2}$ or $1.0x10^{-2}$ appears appropriate. Overall, it can be concluded that the middle row of the table presents the best estimate for cognitive performance in fault scenarios. It should be noted that this is a considerably narrower distribution than the *a priori* distribution postulated for the empirical HRA study put forward in Ref. 115 by Bye *et al*.

55 I consider that the estimated range for cognitive performance suggested by the probabilities reported in the available literature is considerably more conservative than those offered by THERP. Based upon the Halden work in particular, I further suggest that there is little evidence to support the notion of diagnosis being a function of time and considerably more to support it being a function of complexity. This, in turn, appears to be a function of the number of coincident faults being addressed and the presence of misleading indications due to faulted instrumentation.

Assessment of Dependency

Identification of Good Practice in the Treatment of Human Error Dependence

Introduction

56 My regulatory expectations for the treatment of HED are cited principally in TAG T/AST/063 (Ref. 7) on HRA. However, I also undertook a review of available literature to establish current international expectations in this area, to inform my judgements.

IAEA

57 The IAEA sets out its expectations for the treatment of human error in PSA in IAEA Safety Standards Series SSG3 – 'Development and Application of Level 1 PSA for Nuclear Power Plant' (Ref. 116). This identifies that, although techniques used for HRA have improved in recent years, the state of the art in the area is still evolving and as such classical static representation of human behaviour in level 1 PSA can be considered to provide good practice. This suggests that first generation HRA approaches, such as those provided by THERP and HEART (Ref. 113) as opposed to more dynamic modelling approaches such as those provided by expert system based HRA techniques, e.g. Information, Decision and Action in Crew context (IDAC) (Ref. 117) can, at this time, be

considered adequate for use in PSA. The report further highlights the requirement for a treatment of dependency based on the assessment of all PSA cutsets that contain multiple human failure events. Where cutsets containing multiple human errors are found, IAEA requires that an assessment should be undertaken to identify the degree of dependence between the human errors identified and to adjust the HEPs based on this. Within IAEA TECDOC 1151 (Ref. 118), IAEA identify that the degree of dependence between *HFE*s in an accident sequence or cutest is affected factors including:

- Use of common cues.
- Responses called for in the same procedure.
- Closeness in time of cues or required actions.
- Increased stress caused by failure of the first response.

United States Nuclear Regulatory Commission

58 The US NRC in NUREG 1792 (Ref. 119) also identify good practice with respect to HRA. With respect to dependency it is identified that dependency analysis should be undertaken between:

- Pre-initiator human errors and recovery human errors.
- Recovery human errors where there are multiple recoveries available.
- Pre-initiator human errors, where different pre-initiators may be subject to the same common cause human error.
- Post-initiator human errors.
- Post-initiator human errors and recovery human errors.

59 The document also identifies that the minimum HEP value for the *HFE*s in a single fault sequence should not be below x10^{-4} to x10^{-5} range. This indicates the need for, but does not specify the use of, HPLV to limit the claims made on human operator reliability.

60 US NRC also recommends that dependency is accounted for in values used for screening and best estimate analyses. Therefore, some initial estimates of dependency may be required at screening or, alternatively screening values should be sufficiently conservative to encompass the possible effects of dependency or complete dependency should be assumed amongst multiple human errors, particularly recovery human errors.

61 In NUREG 1792 (Ref. 119) US NRC provides specific advice on the factors that contribute to dependency between *HFE*s. The factors identified are:

- The same crew member(s) is responsible for the acts.
- The actions take place relatively close in time such that a crew “mindset” or interpretation of the situation might carryover from one event to the next.
- The procedures and cues used along with the plant conditions related to performing the acts are identical (or nearly so) or related and the applicable steps in the procedures have few or no other steps in between the applicable steps.
- Similar PSFs affect the actions.
- The acts performed are similar manner.

Annex 4

Work Stream 2 Supporting Analysis

- The acts are performed in or near the same location.
- The interpretation of the need for one action might bear on the crews' decision regarding another action, i.e, the basis for one decision in a scenario may influence another decision later in the scenario.

62 Whilst NUREG 1792 (Ref. 119) does not prescribe the use of any particular technique for the treatment of dependency, its advice regarding how levels of dependence should be allocated based on assessment of the above factors, suggest the use of a levels of dependency assessment akin to that provided by THERP, where dependence is assessed at five separate levels (zero, low, moderate, high and complete).

63 *"The more the above commonalities and similarities exist, the greater the potential for dependence among the HFEs (i.e., if the first act is not performed correctly, there is a higher likelihood the second, third... act(s) will also not be performed correctly; and vice versa if the act(s) are successful). For example, if nearly all or all of the above characteristics exist, very high or complete dependence should generally be assumed. If only one or two of the above characteristics exist, then analysts will need to evaluate the likely strength of their effect and the degree of dependence that should be assumed and addressed in quantification".*

64 A follow up report to NUREG 1792, NUREG 1842 (Ref. 120), provides a review of HRA techniques commonly used in the US and assesses each of these against the good practices identified in NUREG-1792 (Ref. 119). The techniques reviewed in the report are:

- THERP.
- ASEP.
- HCR/ORE (Ref. 35).
- Cognitive Based Decision Tree (CBDT) (Ref. 121).
- Electrical Power Research Institute Human Reliability Analysis Calculator (EPRI-HRA) (Ref. 122).
- Success Likelihood Index Methodology – Multi Attribute Utility Decomposition (SLIM-MAUD) (Ref. 123).
- Failure Likelihood Index Methodology (FLIM) (Ref. 124).
- SPAR-H;
- A Technique for Human Event Analysis (ATHEANA) (Ref. 125).
- Revised Systematic Human Action Reliability Procedure (SHARP1) (Ref. 126).

The report provides a summary of each technique. The summary and a brief evaluation of the treatment of dependency for each of the 10 methods included in the review, is provided in Table A4.4 below.

Annex 4

Work Stream 2 Supporting Analysis

Table A4.4: Summary of NUREG 1842 Dependency Treatment Evaluation for Human Reliability Assessment Techniques

Technique	Dependency Treatment	Dependency Evaluation
THERP	Includes a five level dependence model.	Has a five level dependence model for across subtask dependence, and although explicit guidance is not provided, it can reasonably be generalized to address dependence across human actions in a PRA sequence. (Estimates of the appropriate degree of dependency requires analyst judgment.)
ASEP	Includes a simplified version of the THERP dependence model.	Provides a reasonable, simplified version of the THERP dependence model (but THERP is still recommended when generalizing to address dependence across actions in a PRA sequence).
HCR/ORE	Provides a good conceptual discussion of dependencies that need to be addressed.	Details regarding the sources of dependency are not addressed and specific numeric adjustments are not proposed.
CBDT	The method assumes independence among the various factors represented in the decision trees.	
EPRI HRA calculator*	Version 3 of the software includes a means to facilitate analysis of a variety of dependency issues, but the guidance was still being worked on.	Provides a means to analyze dependencies among combinations of multiple HRA events, though specific analysis guidance was still being worked on.
SLIM-MAUD	Does not include a specific dependency model.	
FILM	Does not include a specific dependency model.	
SPAR-H	Includes a THERP like dependency model with additional attributes.	Dependence model based on THERP dependence data/model, with additional attributes added (notably a decision tree to assign the level of dependence). THERP like dependence model can be used to address both subtask and event sequence dependence.
ATHEANA	Consideration of dependencies are included as part of the modelling of the affect of context on performance.	Specific quantitative values are not provided.
SHARP1	Includes a thorough discussion of dependency issues, but does not include quantitative values.	

Annex 4

Work Stream 2 Supporting Analysis

65 The report concludes that *"Appropriate treatment of a variety of potential dependencies is important in modelling human performance, but only few methods have explicit models to support quantification of dependencies. Those with explicit models are all based on THERP, and they are somewhat limited in terms of the range of dependencies they explicitly cover"*.

NASA

66 The US National Aeronautics and Space Administration (NASA) in 2006 also produced a review of HRA methods with an emphasis on those that can support PSA (Ref. 127). Amongst the review criteria that were used to evaluate HRA methods was whether the method provided for explicit treatment of task error dependencies. The NASA review considered 14 HRA methods listed below:

- THERP.
- ASEP.
- SLIM.
- Cognitive Reliability and Error Analysis Method (CREAM) (Ref. 128).
- HEART.
- Nuclear Action Reliability Assessment (NARA) (Ref. 129).
- ATHEANA.
- Connectionist Assessment of Human Reliability (CAHR) (Ref. 130).
- SPAR-H.
- University of Maryland Hybrid (UMH) (Ref. 131).
- Cognitive Error Search and Assessment (CESA) (Ref.132).
- Human Factors Process Failure Modes and Effects Analysis (HFPFMEA) (Ref. 133).
- Time Reliability Correlation (TRC).
- CBDT.

67 The NASA review concludes that only a limited number of HRA methods deal explicitly with dependency and, of those, not all provide a method for deriving conditional HEPs. The techniques that are identified as having a capability to account for dependency are: THERP; ASEP; ATHEANA (qualitative treatment only); SPAR-H; UMH (by selection of PSFs); and CESA. The review identifies that where a technique provides an explicit method for adjusting HEPs, it is the THERP dependency model provides the basis for the calculation procedures.

Annex 5

Work Stream 5 Supporting Analysis

Introduction

1 This annex presents additional details of my Work Stream 5 assessment of plant-wide ergonomics of the UK EPR. This work stream complements the Work Stream 1 detailed consideration of substantiation of human based safety claims by taking a more holistic consideration of the general ergonomics across the whole plant to ensure that it matches modern standards. It is an important element in my consideration that the plant design is ALARP from an HF stand point.

2 My assessment has been based on assessment of the documentation provided by EDF and AREVA for Step 4, along with my detailed observations of the FA3 EPR simulator at CNEN, Paris and from discussions with EDF and AREVA staff during several visits to CNEN. My findings relevant to Step 4 are presented in the Section 4.6 of the main report.

PICS Display Formats

3 Any format can be called up to any PICS workstation or onto the POP. All formats have the same header which permits navigation and alarm handling. Formats are of three types:

- Status displays – which provide information about the condition of the plant.
- Procedural displays - which present instructions on the performance of plant actions.
- Control displays – which permit action on plant equipment.

Annex 5

Work Stream 5 Supporting Analysis

Figure A5.1: Example Display Format Showing the Feed System

[redacted]

Appearance

4 A typical status format is shown in Figure A5.1. The example shows a typical mimic format using colours and symbols as described in Ref. 144.

5 The layout is clear and uncluttered and is arranged with the process flow from left to right in conformity with guidelines. The symbols are clear and self-evident, though it can be argued that the three dimensional shading is unnecessary and may provide excessive clutter. There is clear demarcation of components and parameters. The choice of colours in the displays is acceptable from the examples I have seen, but I would like to see a table of colour usage in a definitive style guide in order to ensure that best ergonomics practice is followed.

6 Text usage, fonts and styles appear consistent so far as I could judge during the simulator presentations and in the examples provided in the supplementary documentation. I did observe that character heights appeared to be smaller than current ergonomics practice would recommend for the expected viewing distance. I consider that it is important that any change in status indicated by colour change, should also be supported by an additional visual cue, typically a shape change. A good example is shown in Figure A5.2, which shows the coding of valves on PICS formats. This confirms that, when a control valve changes status, this is illustrated by both colour and shape change.

Annex 5

Work Stream 5 Supporting Analysis

Figure A5.2: Proposed Valve Symbology

[redacted]

7 Other examples I have noted use colour change as the only cue to a change in parameter status; an instance is the AD indication.

8 Trend displays are available as formats where the operator can select the required parameters. Figure A5.3 is an example of a trend format.

Display Controls and Windowing

9 The primary display has well defined working areas. The header is a permanent area and provides for menu selection and alarm indication. The lower area presents information about plant status or procedural instructions. Secondary windows are used for control plaques, which appear in a fixed position and they are clearly superimposed on the primary window.

10 The mouse is used for the control of formats and not the keyboard. One keyboard is used for data entry on any of the five screens. Data entry is obviously achieved where the focus is provided that a data entry field is present. One mouse can move the cursor over the five displays.

Figure A5.3: Example Trend Format

[redacted]

11 There are various types of target for the mouse on the PICS formats, such as menu selection, control activation and display navigation. The drop-down menus on the header provide immediate access to navigation options and, in addition, direct pointers allow access, via labelled hot links, to formats related to the current display. I noted a possible lack of consistency in marking mouse sensitive areas (“hot-spots”) on the formats.

Navigation

12 The main navigational features are provided by the header bar which gives immediate access to a range of options. These options are displayed as icons, the meaning of which will need to be learned by the operator. However, this is not seen as arduous and each icon is supported by contextual menus.

13 A hierarchical display structure is under development and the menu selection, which is planned but still under development, will permit direct access to any format. There is a back button to recall the last page in the event of a mis-selection. Each format is provided with hotlinks to relevant, related formats.

Controls

14 Controls are only active from a workstation set in control mode. Two workstations only can be in control mode and these would normally be the OS and OA workstations. The SS or spare workstation would only be set to control mode in the event of a workstation failure.

15 Controls are accessible as superimposed control plaques directly from the status formats and the respective control access points are grouped, as necessary, on appropriate formats. To control an item, the operator uses a mouse click to address the control

Annex 5

Work Stream 5 Supporting Analysis

element, pump or valve etc. and the appropriate plaque appears as a superimposed modal window, see Figure A5.4.

Figure A5.4: Example Control Plaque for a Valve

[redacted]

16 Only one control plaque can be controlled at a time on any one display. The control plaque provides the necessary facilities for operating an equipment item. The actions are initiated by standard '*windows*' control buttons; where necessary there are radio buttons and check boxes. The various options which are available are indicated in light grey and options, not available, are shown in dark grey. In Figure A5.4, the valve is in '*auto'* mode and the option to dismiss the plaque and to call up associated trends are active. Any action is confirmed by the '*execute*' key. The control display items change to provide feedback that an action has been carried out.

17 When entering a numerical value, the value must be within a specified range or it is not accepted and this is indicated to the operator. After entering an acceptable value, the changed value must be validated and then executed, so there are two checks on the required parameter change. Where appropriate, alarm indications can be shown on the control plaque to draw the operator's attention to any anomalous values.

18 Automatic sequences are driven from appropriate PICS formats. The formats provide information as to the status of any automated sequence and the operator can further interrogate detailed status displays to investigate the logic of the sequence if necessary.

SICS Operation

19 During normal operations the SICS instrumentation including indicators and alarms is active, but the controls are disabled. The controls can only be activated if control from PICS has been cancelled. SICS has the following functions:

Annex 5

Work Stream 5 Supporting Analysis

- Substitute control of the plant during scheduled maintenance of PICS. In this case the plant is maintained in steady state using SICS until PICS is returned to service.
- Control of the plant in the event of PICS failure. In the case of an unexpected failure of PICS, SICS provides alternative control. The plant can be maintained in steady state for a pre-ordained time period (this duration would be a licensing issue), if the PICS cannot be restored within this period, then SICS is used to bring about a safe shutdown.
- Diverse and redundant plant supervision during an accident/incident. If the plant enters a condition in which the AD is activated, then the SICS panel is used to independently verify the state of the critical safety functions. Initially, this is carried out by the SS and then by the SE when he/she arrives at the MCR. In this mode, the normal SICS mode, the instrumentation and alarms are all “live” but the controls are not activated. The SS and SE use a printed procedure to assess SOA status from the SICS panels.
- Safe, controlled shutdown if PIC fails during an accident/incident scenario. If the PICS fails during an incident/accident, then the SICS controls are activated and the OA and OS move to the SICS panels and operate the plant completely from the SICS. They use a tailored set of procedures, similar to the PICS printed procedures, for selecting an appropriate strategy and then bringing the plant to a safe condition.

20 The decision to transfer over control from the PICS to the SICS is taken after a PICS diagnostics phase to examine criteria, which are pre-defined by a procedure. SICS is designed so that the transfer of operation from the PICS to the SICS can be performed whatever the condition of the plant unit. The use of the SICS is supported by tailored paper procedures. *When MCP [PICS] is unavailable, operating staff use MCS [SICS] and the situation is managed through incident and accident operating procedures. It is not necessary to create alarm sheets for MCS [SICS]* (Ref. 149).

Alarm Presentation in the MCR

21 The presentation and operation of the alarm system is described in detail in the November 2009 PCSR (Ref. 17), as noted above. The specification of the functionality of the alarm system is described in detail in Reference 148. The operation of the alarm system was demonstrated during the simulator visits and these presentations are summarised in Ref. 153. The information regarding alarms on the SICS panel is provided in the SICS specification (Ref. 149).

<u>PICS Alarms</u>

22 The main alarm system is delivered onto the computerised displays controlled by the PICS. There is no permanent alarm display, the alarm lists are formats which are called up by operators as required. There is no requirement, currently, that any alarm format should be on permanent display, either on the local operator work stations or on the POP. If an alarm condition arises, then this is announced by an audible signal tone and a flashing icon on the general format header. This header is on all display formats at all workstations and on the POP. Alarms are categorised into four priority levels, increasing in severity from 1 through to 4. If a Priority 4 alarm occurs this, by definition, indicates a

Annex 5

Work Stream 5 Supporting Analysis

CI (Incident Mode) or CA (Accident Mode) condition which triggers the onset of the AD system. The onset of AD is signalled by a specific audible chime. Thereafter, individual alarm signals are not used as the operating crew adopt the appropriate SOA as prescribed by the AD system. It was noted in the simulator demonstration that the OS and OA would expect to respond to alarms if it judged it appropriate when they had some unoccupied time during execution of SOA actions. Alarm information, although not crucial to managing the plant, could provide useful information on plant condition.

SICS Alarms

23 In the event of a PICS failure, operation is transferred to the SICS hard-wired panel. The SICS provides a suite of instrumentation, which is intended to be sufficient for operators to bring about a safe shutdown of the plant. It is not used for at-power operation. The SICS is provided with traditional alarm annunciators, i.e. trans-illuminated alarm tiles, which are located at appropriate locations on the panels. As listed in Ref. 42, there are approximately 250 SICS alarm annunciators. These are set in groups related to the plant section controls and displays. When using SICS, the situation is managed through written incident and accident operating procedures. It is not yet clear whether there will be an additional set of printed alarm sheets for use when operating with the SICS.

The Alarm System Interface

24 The MCR alarm interface is centred on the PICS and is a typical computerised interface with flexible and intuitive features. The alarm information is available at all workstations and at the POP.

The Alarm Header

Figure A5.5: The Alarm Header – as Shown on Every Pics Display Format

[redacted]

25 The header, which is shown on every PIC format is shown in Figure A5.5. The right hand section indicates alarm status. The header provides a summary of key information on the number of alarms and their priority. Any flashing icon indicates that there are unaccepted alarms. A mouse click on the icon immediately brings up a drop-down menu from which the operator can select various optional displays of the alarm list format. These include:

- General alarm list.
- Alarms by category/priority.
- Inhibited alarms.
- Alarms under maintenance.

The Alarm List

26 Figure A5.6 shows an example alarm list. The list displays each active alarm as a delineated block. The leftmost icons show the status of the alarm, followed by the alarm code and then the alarm description. This is a typical style of alarm presentation and has the benefit that the interface allows the operator to readily select lists of separated alarm

Annex 5

Work Stream 5 Supporting Analysis

categories, including priorities, filtered or unfiltered alarm lists and inhibited alarms. It should be noted that alarm information is not embedded in the process status displays. However, appropriate alarms are shown in the control plaques.

Figure A5.6: An Example of an Alarm List

[redacted]

Figure A5.7: An Example of an Alarm Sheet

[redacted]

Annex 5

Work Stream 5 Supporting Analysis

27 Figure A5.7 shows an example an alarm sheet. There is an alarm sheet for each possible alarm. The sheet can be obtained directly from the alarm list by a single click on the corresponding line in the alarm list.

28 The sheet provides details about the alarm which includes possible causes, actions to be taken, and consequences. The information for each alarm is limited to a one page screen format. In addition, it provides direct links to the relevant plant operation displays where appropriate remedial action can be taken.

29 The alarm sheets are intended to supply the all information required for the operator to interpret and manage the unexpected events signalled by an alarm. They present:

- The cause of the alarm, i.e. the likely fault initiating the alarm.
- Indicate the operational procedure to follow.
- Indicate the functional consequences and associated risks due to the fault.
- Allow the operator to access the necessary control or status formats so that they can check automated actions and to execute any actions defined in the operational procedures.

The Alarm Audible Signals

30 There are the following audible signals planned for the MCR:

- A short series of repeated tones which indicate onset of an alarm; there are no different tones for the four priorities. The alarm onset tone sequence can be silenced at the configured operators console; this is accomplished by clicking on the “Horn off” button which is provided on all screen display headers. The simulator also permits all tones to be silenced but this may not be applied in the actual plant. The intention is that the operator will be able to silence all audible signals in the MCR but only when the plant is in CIA mode, i.e. when the AD system is in operation. This audible signal inhibition will be automatically re-set when the plant returns to normal condition.
- There is single chime which occurs when an alarm condition returns to its normal condition.
- There is a specific alarm chime which indicates that the AD system has activated. This is readily distinguished from the alarm onset chime. This can be silenced at the operator workstation.
- There are, in addition, ‘Voiced’ messages which are activated to draw attention to the transition of the plant to a different status, for example Reactor Trip. Each message is presaged by a chime and the message is repeated.
- There is an additional audible signal for fire alarms. Ref. 2 states that: *“The fire-alarm cabinet normally uses an audible signal for fire alarms that is sufficiently identifiable to alert the operators. This audible signal is very different from the sound used for conventional alarms.”.* This alarm was not available for demonstration at the simulator facility.

Annex 5

Work Stream 5 Supporting Analysis

Work Organisation

Operating Modes

31 Four operating modes are defined for the EPR. These are:

- CN - Normal operating mode.
- CI - Incident mode.
- CA - Accident mode.
- AG - Serious accident management.

32 CN represents the normal, everyday operating mode. The crew's role is to adjust plant conditions in order to maintain power production as safely and as efficiently as possible. Any changes in plant conditions are generally in response to operator action to initiate process control functions. CI, CA and AG modes bring about a fundamental change in the relationship between the operator and the plant because unit conditions are no longer dependent so much on operator action but on abnormal equipment and plant conditions with associated increasing degrees of severity. The conditions where mode CA and mode CI exist together are known as mode CIA.

33 At the onset of these modes, automatic changes will be undertaken by the automation system without any operator intervention. The operators are "*in second place*" (November 2009 PCSR Ref. 17), and their prime role is to supplement any automatic actions to bring about a return to safe and normal plant conditions. In my view, for the crew, the principle distinction between operational modes appears to be between CN on the one hand, and CI, CA and AG on the other. The key distinction being that in the CN mode plant conditions only change as a consequence of operator actions. In contrast, the CI, CA and AG modes are all concerned with abnormal conditions to some degree of severity. This is borne out by the documentation which tends to refer to the combination of CI and CA as the CIA mode. Furthermore, as the November 2009 PCSR (Ref. 17) points out, *"AG mode need not be treated separately since, from the organisational viewpoint, it does not have any specific characteristics which require the shift crew to adopt measures which are different from those taken in CIA mode.".* The operational organization has, accordingly, been based on dealing with the two modes: CN and CIA.

MCR Operating Team

34 The proposals for the MCR staffing follow these principles:

- Ensuring adequate workload in any operational mode, the individual should not be overloaded with activities but should be kept occupied.
- There should be a clear assignment of duties.
- The organization is strongly based on OEF. The general role for EPR operators is the same as for the other French plants, except where it must take account of implications of the design changes in EPR.

35 In the current plants, there is a secondary side operator and a reactor operator. OEF suggested that in CIA mode, the secondary side operator had relatively little to do and, with the increased automation in EPR, this workload would be further reduced. On the other hand, the reactor operator has a much heavier workload and in a fast moving situation they have little opportunity to *"obtain an overall picture of operating activities..."*

Annex 5

Work Stream 5 Supporting Analysis

(Ref. 69). A simulator-based study, which included observation of experienced crews managing scenarios combined with interviews and discussions (Ref. 48) concluded that the duties of the two operators should be re-assigned with both taking over more overall plant responsibilities, but with one being focussed on strategy and the other one carrying out required actions.

36 The proposed MCR staffing comprises a SS and two operators. This complement is supported by a SE in the event of plant disturbance. The main change from current plants is the way responsibilities are divided between the two operators. These are now termed OS and OA and they no longer have separate responsibility for the reactor and the secondary side. Both OS and OA have similar training and experience and they are both fully qualified operators. Typically, it is expected that OS and OA will be designated at the start of a shift and these roles will remain for the duration of that shift. There is also the option that the particular skills of the operator will determine designation to OS or OA role.

Supervisor

37 The SS is leader of the team and responsible for the team activities as a whole. In the documentation, this role is sometimes termed Shift Supervisor, Control Room Supervisor or Shift Manager. The SS role corresponds to the Control Room Supervisor in a UK power station and so the SS is senior to the operators, but is not to be confused with Shift Charge Engineer. The SS duties are centred on the MCR and, particularly in CIA mode, the SS is involved in key decision making. The SS is responsible for the management of the crew and keeps track of all operating activities to ensure compliance with safety requirements. The SS is responsible for assessing the safety of the units and these duties cannot be delegated.

Strategy Operator

38 The OS enforces the operating strategy and monitors the unit condition but takes little or no direct control action. The OS is responsible for planning and scheduling the actions that the OA will undertake. The OS also monitors the OA’s progress and completion of actions and monitors key process parameters in order to detect abnormal conditions. In CIA mode, the OS selects the strategy to be applied based on plant status, using the AD function. The OS is also alerted by the system if the status changes and requests the OA to perform actions as appropriate to the prevailing strategy.

Action Operator

39 The operator designated as OA for a shift will follow the instructions given by the OS. Thus the OA performs most process actions.

40 In CIA mode, the OA performs actions in accordance with strategy chosen by the OS (and guided by the AD) and applies methods and procedures, using PICS command and status formats. The OA reports to the OS on the completion of these actions. In addition, the OA requests field operators to perform local-to-plant actions and performs first-level monitoring of systems. Importantly, the OA, can, if necessary, run through and check the initial orientation checks within a strategy in order to support OS at the onset of an incident.

Annex 5

Work Stream 5 Supporting Analysis

Safety Engineer

41 In normal mode, the SE has duties not necessarily related to the MCR. The SE is on call and can be called out to attend by the operating shift crew. On initiation of CIA mode and activation of the DA, the SE should be summoned to the MCR by the SS. SE must be able to reach the MCR within 40 minutes of being requested. He then performs independent verifications of the plant status, based on paper-based SOA procedures and the SICS panel. The SE is not required to operate the plant. This provides an independent check of plant status separate from information presented by the PICS and the DA.

Procedures

Intended Operation of SOA

AD Activation

42 The AD system continually monitors plant status during all phases of operation. Under any of the conditions listed above, the interface to the system becomes active and, upon initiation, the AD icon in every PICS format header is illuminated red and flashes. In addition, AD initiation activates a specific audible alarm. As with the rest of the alarm system, the operator acknowledges AD onset and the icon becomes steady and the audible signal is silenced. The operator then uses the AD overview format which is shown in Figure A5.8. I note from Ref. 148 HMI, that when the AD is activated, after acceptance, there is no additional signal beyond the red colour to indicate that activation has occurred, see Figure A5.9.

43 The AD overview format is divided into two vertical panes. The left pane presents the status of the six Critical Safety Functions. At the top are the three functions associated with the primary side: core sub-criticality, RCS water inventory, and primary side heat removal. In the centre are the secondary side functions, steam generator integrity and water inventory. At the bottom is containment integrity. The right pane provides advice to the operator as to the strategy to be carried out to mitigate the threat(s) that the AD has identified/diagnosed to the various functions. This includes identification of the written procedure(s) to be used together with hot links to the appropriate system formats.

Annex 5

Work Stream 5 Supporting Analysis

Figure A5.8: The Automatic Diagnosis (AD) Overview Display

[redacted]

Figure A5.9: The Automatic Diagnosis (AD) Alerting Icon

[redacted]

Immediate Actions

44 At the onset of an emergency situation, it is intended that the crew will adopt the SOA. Upon AD activation, the intention is that the Strategy Operator (OS) will select the appropriate strategy procedure and the Action Operator (OA) will select the corresponding action procedure. Both of these are structured A3 size, paper documents. The supervisor (SS) is informed of AD activation and he/she will summon the Safety Engineer (SE) who is permanently stationed so that he/she can be on duty within the MCR within 40 minutes. The SS and the two operators confirm the strategy to be undertaken. There is no requirement for diagnosis, the AD overview indicates which

Annex 5

Work Stream 5 Supporting Analysis

strategy should be adopted and provides a summary explanation of the reasons for taking the prescribed action in terms of the information relating to the six critical functions.

Subsequent Remedial Actions

45 The OS and the OA adopt the strategy of operations as indicated by the written procedures and implement them. The OS maintains an overview of the implemented strategy while the OA carries out the specific actions as required. The intention is that the workload of the two crew members is equivalent. Once the AD is activated, the OA and the OS ignore the alarm system and they will silence the alarm audible signals. The function of AD is intended to render the use of the alarm system unnecessary. However, it was noted during the simulator presentations that the OS may have the opportunity during low activity periods to review the alarm list and accept any unaccepted alarm messages.

46 In the meantime, the SS undertakes an independent and diverse check of the status of the plant based on SOA using the SICS with a corresponding paper-based procedure. The SS continues with this activity until the SE arrives. The SE then continues this independent check until the plant is restored to a safe condition. The SE and SS do not take any operational actions; this is exclusive to OS and OA.

Alternative Strategies and Strategy Change

47 If the AD detects that the initially selected remedial strategy is not correcting the situation, or if a change to critical function status occurs, then it will select an alternative strategy. This is announced by re-activation of the flashing AD icon on all format headers, and re-initiation of the audible alarm. The OS and OA then terminate the current strategy and its associated actions and select the notified changed strategy. The SS will be immediately informed. It is noted that once AD has triggered, the operating team must follow the recommended strategy. If they believe that the AD is incorrect, or if the SE reports an anomaly when monitoring the SICS panel, then they consider revising the AD strategy. I note that, as well as confirming SOA status using SICS, the operators can interrogate subsidiary formats to the AD overview in order to investigate the various component computations from which the AD strategy is derived. These formats are addressed directly from the AD overview and they provide a graphical indication of the way the AD solution has been determined. However, not following the AD recommended strategy is a serious decision and this would require careful and systematic consideration and appropriate authorisation by the supervisor.

SOA Paper-based Procedures

48 Once the AD has activated, the operations are regulated and controlled by paper–presented procedures. There is a paper procedure for each of the strategies that may be requested by the DA. Each procedure is in two forms, one for the OS and one for the OA. It should be noted that there are no different PICS formats for OS and OA. The OS and OA procedures are carefully structured, A3 format paper documents which are colour coded and make extensive use flow charts. They include references to the various display formats which must be used to implement control actions. They are always available in the MCR. An example is shown in Figure A5.10.

Annex 5

Work Stream 5 Supporting Analysis

49 The procedure describes the strategy and the required actions. These actions are determined on the basis of criteria relating to the status of physical parameters or the status of components.

50 The strategy is generally presented as a set of comprehensive logic diagrams plus references to the appropriate process status formats. The procedure directs the operators to track the key parameters that could change and to display the correct operational views. This means that the operator is already prepared to intervene in the process as necessary.

Figure A5.10: Example of a Paper-based OS Procedure

[redacted]