Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Human Factors Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-012
Revision 0
11 November 2011

.

COPYRIGHT

First published December 2011

PREFACE

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

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000® 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 Westinghouse 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 AP1000® reactor.

EXECUTIVE SUMMARY

Introduction

This report presents the findings of the Human Factors assessment of the AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's Generic Design Assessment. The assessment has been carried out on the Pre-construction Safety Report and supporting documentation submitted by Westinghouse during Generic Design Assessment Step 4.

The 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 report was more aligned to a Generic Design Assessment Step 2 report; focusing on consideration of Westinghouse's safety claims, with some 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 (Ref. 1).

Scope of assessment

The following items have been agreed with Westinghouse as being outside of the scope of Generic Design Assessment (Phase 1) for Human Factors:

- Detailed procedure design;
- Final human machine/computer interface designs;
- Work organisation;
- Staffing levels; and
- Administrative controls.

My assessment has focused on five work streams:

Work Stream 1 - Substantiation of Human Based Safety Actions

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. 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 qualitative 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; and

- 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 development of the design and its safety assessment.

Work Steam 2 - Generic Human Reliability Assessment

Work Stream 1 aims to assess in detail the substantiation of the Human Reliability Assessment, and to a certain extent Work Streams 5 and 3 also support the assessment of the Human Reliability Assessment substantiation. Work Stream 2 aims to look generically at particular aspects of the Human Reliability Assessment across the safety submission, particularly relating to Human Reliability Assessment methods and application, and has a more quantitative focus. Work Stream 2 also continues the assessment of the Human Reliability Assessment carried out for Generic Design Assessment Step 3 from both the Probabilistic Safety Analysis and Human Factors technical areas.

Work Stream 3 - Engineering Systems

This area has two main assessment components;

- system/equipment maintenance - including inspection, calibration and testing (at a strategic level - for example the general approach to 'maintenance'). Linked to Work Streams 1 and 5; and
- consideration of 'novel' engineering systems - for example the Automatic Depressurisation System. My focus relates to the uncertainty of the practical maintenance and operation of such systems in reality.

This work stream is important to ensure claims and assumptions about the reliability of systems and components are adequately underpinned.

Work Stream 4 - Human Factors Integration

The focus of this work stream is on the general processes and mechanisms in place to deliver quality Human Factors input to the design of the UK AP1000 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 me with a level of confidence or otherwise that the Human Factors analyses not assessed during Generic Design Assessment are of a suitable quality to inform the design and safety submission, and ultimately to support reliable human intervention.

Work Stream 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 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.

Conclusions

My principal conclusions in these areas are:

Work Stream 1 - Substantiation of Human Based Safety Actions

In general I judge that Westinghouse has applied themselves to the problem of Human Factors substantiation, and have identified some sources of operator failure that were omitted by the Probabilistic Risk Assessment. Westinghouse has captured and incorporated some valuable Utility input, together with some potentially useful error reduction strategies, and some of the human based safety claims seem reasonable.

There are 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 AP1000 progresses beyond the Generic Pre-construction Safety Report stage.

Westinghouse submitted a significant volume of important Human Factors analysis towards the end of Generic Design Assessment Step 4, relating to Regulatory Observations in the areas of human error mechanisms, operator misdiagnosis and violation potential. However as this material was submitted in December 2010, I was only able to undertake a very high review of the submission to gain confidence in the approach; I was not able to undertake a detailed and thorough assessment within the Generic Design Assessment Step 4 timescales. I have therefore raised a Generic Design Assessment Issue to reflect the significant gap in the safety case that these Regulatory Observations represent. The Generic Design Assessment Issue Action requires Westinghouse to support the Office for Nuclear Regulation's full assessment of this submission.

Work Stream 2 - Generic Human Reliability Assessment

It is clear that there are many and considerable issues with the current AP1000 Human Reliability Assessment. Both myself and my Probabilistic Safety Analysis colleague highlighted problems with the model at the end of Generic Design Assessment Step 3, and the work that I have undertaken during Generic Design Assessment Step 4 has amplified my judgement that the Human Reliability Assessment should be fully revised. I recognise that the qualitative Human Factors assessment work undertaken by Westinghouse to develop the Human Factors safety case for the AP1000 has not been reflected in the Human Reliability Assessment; and as the safety case and supporting risk assessments move forward those analyses should be fully incorporated to the revised Human Reliability Assessment model. I question the general applicability of the Technique for Human Error Rate Prediction and early consideration should be given to the appropriateness of the Technique for Human Error Rate Prediction to the revised Human Reliability Assessment. I do not consider that the current model represents recognised good practice in terms of quantitative Human Reliability Assessment, and that this is largely a result of the age of the model; its incompleteness and all of the modelling issues that I highlight in this report.

Work Stream 3 - Engineering Systems

In general I judge that Westinghouse has made a good start in addressing the human reliability aspects of maintenance; and there is evidence of analysis and design input to support their claims in this area. However there are significant gaps in the Human Factors contribution that I am taking forward as part of Generic Design Assessment Issue Action HF1.A1.

Work Stream 4 - Human Factors Integration

In general I judge that Westinghouse has evidence of a Human Factors Engineering programme of work; but it is just that; a Human Factors engineering scope of work, which is in itself limited by their programme and resource split into core, adjunct and peripheral elements. This split is risk based and does not take explicit account of complexity and novelty; and in my opinion this approach does not necessarily result in an As Low As Reasonably Practicable position. 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 Human Factors Integration programme are evidenced; there are significant omissions. This is to be addressed by a licensee as part of a site specific Pre-construction Safety Report.

Work Stream 5 – 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) is adequate and will not significantly undermine human reliability. I note many observations across the assessment area and these are cited as Assessment Findings to be addressed post Pre-construction Safety Report.

Overall Conclusions

Overall, Westinghouse has undertaken a significant volume of quality Human Factors assessment work to support their Generic Design Assessment submission for Human Factors. Westinghouse has applied considerable competent resource to improve its position on Human Factors from that at the end of Generic Design Assessment Step 3. My interactions with Westinghouse's team have been positive, and through regulatory intervention and a willingness by Westinghouse to understand the UK regulatory system and safety case regime, its achievements in Human Factors at the end of Generic Design Assessment Step 4 are to be commended.

There are gaps in the Human Factors safety case; some of which are safety significant and have resulted in a Generic Design Assessment Issue. However Westinghouse has delivered analyses to address these concerns; although the timing of these did not allow me to fully consider them within Generic Design Assessment Step 4.

The majority of my conclusions are cited as Assessment Findings to be taken forward as routine regulatory business post Generic Pre-construction Safety Report. This reflects my judgement that in the Human Factors technical area, based on my assessment, there is a minimal risk to progression of the Generic Pre-construction Safety Report. Should subsequent assessment reveal further deficiencies in the design or safety analysis, typically Human Factors solutions can 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 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

AC	Alternating Current
ADAMS	Agencywide Documents Access and Management System
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
ANS	American Nuclear Society
AoF	Allocation of Function
AOP	Abnormal Operating Procedure
APoE	(HEART) Assessed Proportion of Effect
APS	Alarm Presentation System
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BMS	Business Management System
BSL	Basic Safety Level
BSO	Basic Safety Objective
CAD	Computer Aided Design
CCS	Component Cooling System
CCTV	Closed Circuit Television
CCW	Component Cooling Water
CDF	Core Damage Frequency
CHEP	Conditional Human Error Probability
C&I	Control and Instrumentation
CIM	Component Interface Module
CMT	Core Makeup Tank
CNSC	Canadian Nuclear Safety Commission
COL	Combined Operation License
COMIT	Constructability, Operability, Maintainability, Inspectability and Testability
COTS	Commercial Off The Shelf
CPS	Computerised Procedure System
CSF	Critical Safety Function
CVS	Chemical Volume Control System
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DBA	Design Basis Analysis
DCD	Design Control Document

LIST OF ABBREVIATIONS

DCP	Design Change Process
DCIS	Distributed Control and Information System
DCR	Design Confirmation Rule
D-RAP	Design Reliability Assurance Program
ECCS	Emergency Core Cooling System
EEMUA	Engineering Equipment and Materials Users' Association
ELS	Emergency Lighting System
EOP	Emergency Operating Procedure
EPC	(HEART) Error Producing Condition
ERG	Emergency Response Guidelines
ESF	Engineered Safety Feature
FBTA	Function Based Task Analysis
FHS	Fuel Handling System
FMEA	Failure Modes and Effects Analysis
FSER	Final Safety Evaluation Report
FV	Fussell Vesely
GDA	Generic Design Assessment
HAD	Human Action Database
HAZOP	Hazard and Operability study
HCI	Human Computer Interaction
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
HFEPP	Human Factors Engineering Programme Plan
HFI	Human Factors Integration
HFIP	Human Factors Integration Plan
HMI	Human Machine Interface
HPLV	Human Performance Limiting Value
HQ	Headquarters
HRA	Human Reliability Assessment
HSE	Health and Safety Executive
HSI	Human System Interface

LIST OF ABBREVIATIONS

HTA	Hierarchical Task Analysis
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IRWST	In-containment Refuelling Water Storage Tank
ISV	Integrated Systems Validation
ITAAC	Inspection, Tests, Analyses, and Acceptance Criteria
JTA	Job and Task Analysis
LAN	Local Area Network
LOCA	Loss of Coolant Accident
LERF	Large Early Release Frequency
LRF	Large Release Frequency
MCA	Main Control Area
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme
MMI	Man Machine Interface
MSIV	Main Steam Isolation Valve
MTIS	Maintenance, Test, Inspection and Surveillance
NASA	National Aeronautics and Space Administration (US)
ND	Nuclear Directorate
NOP	Normal Operating Procedure
NPP	Nuclear Power Plant
NRC	(US) Nuclear Regulatory Commission
OCS	Operational and Control Centres System
OD	Outer Diameter
OEF	Operating Experience Feedback
OER	Operating Experience Review
OSA	Operational Sequence Analysis
OSC	Operations Support Centre
OSD	Operational Sequence Diagram
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PCmSR	Pre-commissioning Safety Report
PDSP	Primary Dedicated Safety Panel
PMS	Protection and Safety Monitoring System
POSR	Pre-operational Safety Report
PPE	Personal Protective Equipment

LIST OF ABBREVIATIONS

PRA	Probabilistic Risk Assessment (USA term for PSA)
PREDICT	Procedure to Review and Evaluate Dependency in Complex Technologies
PRHR	Passive Residual Heat Removal System
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
PXS	Passive Core Cooling System
PZR	Pressurizer
QA	Quality Assurance
QMS	Quality Management System
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RIF	Risk Importance Factor
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
RO	Reactor Operator
RSR	Remote Shutdown Room
RSW	Remote Shutdown Workstation
RSWP	Remote Shutdown Workstation Panel
RTNSS	Regulatory Treatment of Non-Safety Systems
SAMG	Severe Accident Management Guidelines
SAP	Safety Assessment Principle
SCE	Shift Charge Engineer
SDM	Shutdown Margin
SDSP	Secondary Dedicated Safety Panel
SER	Safety Evaluation Report
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SMJ	Seismic Monitoring System
SMS	Special Monitoring System
SPAR-	Standard Plant Analysis Risk HRA
SQEP	Suitably Qualified and Experienced Person
SRK	Skills, Rules, Knowledge
SRO	Senior Reactor Operator
SSC	Structures, Systems and Components
SSD	System Specification Document
STA	Shift Technical Adviser

LIST OF ABBREVIATIONS

SZB	Sizewell B
TAD	Target Audience Description
TAG	Technical Assessment Guide
THERP	Technique for Human Error Rate Prediction
TLX	(NASA) Task Load Index
TQ	Technical Query
TRACEr	Technique for Retrospective and Predictive Analysis of Cognitive Error in Air Traffic Control
TS	Technical Specifications
TSC	Technical Support Centre
TSC	Technical Support Contractor
UK	United Kingdom
UPS	Uninterruptable Power Supply
URD	Utility Requirements Document
US	United States
USA	United States of America
VAS	Radiologically Controlled Area Ventilation System
VBS	Non-Radioactive Ventilation System
VDU	Visual Display Unit
VES	Emergency Habitability System
V&V	Verification and Validation
WEC	Westinghouse Electric Company LLC
WENRA	Western European Nuclear Regulators' Association
WPIS	Wall Panel Information System

TABLE OF CONTENTS

1 INTRODUCTION 1
2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR HUMAN FACTORS 2
2.1 Human Factors in Context 2
2.1.1 Human Factors in the Pre-construction Safety Report 2
2.2 Generic Assessment Plan 5
2.2.1 Generic Standards and Criteria 6
2.2.2 Findings from Generic Design Assessment Step 3 8
2.2.3 Additional Areas for Step 4 Human Factors Assessment 10
2.2.4 Research 11
2.2.5 Work Stream 1: Substantiation of Human Based Safety Actions 11
2.2.6 Work Stream 2: Generic Human Reliability Assessment 16
2.2.7 Work Stream 3: Engineering Systems 18
2.2.8 Work Stream 4: Human Factors Integration 19
2.2.9 Work Stream 5: Plant-Wide Generic Human Factors Assessment 20
2.2.10 Regulatory Interactions with Westinghouse 26
2.2.11 Use of Technical Support Contractors 28
2.2.12 Cross-cutting Topics and Integration with Other Assessment Topics 29
2.2.13 Out of Scope Items 30
3 WESTINGHOUSE'S SAFETY CASE 31
3.1 Quantitative Human Reliability Assessment 31
3.2 Qualitative Human Reliability Assessment and Human Factors Engineering 33
3.2.1 Structure and Broad Content of the Human Factors Topic Report 33
3.2.2 Safety Claims 33
3.2.3 Westinghouse Methodology for Development of the Human Factors Topic Report 34
3.2.4 Human Factors Engineering 34
3.2.5 Supporting Data – Appendices 35
4 GENERIC DESIGN ASSESSMENT STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR HUMAN FACTORS 36
4.1 Structure of Section 36
4.2 Work Stream 1: Substantiation of Human Based Safety Actions - Assessment 36
4.2.1 Detailed Assessment of Human Actions 37
4.2.2 Assumptions Testing / Analytical Completeness 47
4.2.3 ALARP Assessment 48
4.2.4 Conclusions 49
4.3 Work Stream 2: Generic Human Reliability Assessment - Assessment 50
4.3.1 Type A Human Error Modelling Method 51
4.3.2 Relevance of Extant Human Reliability Assessment Techniques for the Assessment of Modern Control Room Task Environments 52
4.3.3 Application of the THERP Method and Treatment of Diagnosis in Human Reliability Assessment 57
4.3.4 Assessment of Dependency 65
4.3.5 Conclusions 77

4.4 Work Stream 3: Engineering Systems - Assessment 77
4.4.1 Maintenance / Maintainability 78
4.4.2 Consideration of Novel Engineered Systems 81
4.4.3 Conclusions 83
4.5 Work Stream 4: Human Factors Integration - Assessment 83
4.5.1 Scope of Human Factors Integration (HFI) 84
4.5.2 Integration and Implementation 90
4.5.3 Management, Organisation and SQEP 92
4.5.4 Management of Risks, Issues, Assumptions and Uncertainties 93
4.5.5 Standards Applied and Relevant Good Practice 93
4.5.6 Conclusions 95
4.6 Work Stream 5: Plant-Wide Generic Human Factors Assessment - Assessment 96
4.6.1 Allocation of Function 96
4.6.2 Task Analysis 103
4.6.3 Workstation and Workplace Design 108
4.6.4 Environment 112
4.6.5 Control/Display Interfaces and Alarms 118
4.6.6 Engineering Tests 133
4.6.7 Procedures 134
4.6.8 Staffing and Work Organisation 142
4.6.9 Conclusions 143
4.7 Overseas Regulatory Interface 143
4.7.1 Introduction 143
4.7.2 US Nuclear Regulatory Commission 144
4.7.3 Canadian Nuclear Safety Commission 149
5 CONCLUSIONS 150
5.1 Overview 150
5.2 Assessment Area Conclusions 150
5.2.1 Work Stream 1 - Substantiation of Human Based Safety Actions 150
5.2.2 Work Stream 2 - Generic Human Reliability Assessment (HRA) 151
5.2.3 Work Stream 3 - Engineering Systems 151
5.2.4 Work Stream 4 - HF Integration (HFI) 151
5.2.5 Work Stream 5 – Plant-Wide Generic HF Assessment 151
5.3 Meaningful Generic Design Assessment 152
5.4 Global Judgements on Adequacy 152
5.4.1 Assessment Findings 154
5.4.2 Generic Design Assessment Issues 154
6 REFERENCES 155

Tables

Table 1: Generic GDA Step 4 Assessment Requirements and Human Factors Considerations

Table 2: Safety Assessment Principles and Technical Assessment Guides Used as an Assessment Basis for GDA Step 4 HF Assessments

Table 3: GDA Step 3 Issues Considered Further During GDA Step 4
Table 4: IAEA Error Classifications
Table 5: Human Actions Assessed for the Pilot Assessment
Table 6: Human Factors Regulatory Observations Considered during GDA Step 4
Table 7: Human Factors Meetings and Discussions between ND and Westinghouse during GDA Step 4
Table 8: Cross-cutting Assessment Disciplines with Human Factors
Table 9: Actions of Importance Judged not to have been Substantiated by Westinghouse
Table 10: Actions of Lesser Importance Judged not to have been Substantiated by Westinghouse
Table 11: Core Damage Frequency Impact of Revised (ND Generated) Human Error Probabilities
Table 12: Holistic Task Experimental Studies
Table 13: Object Level Task Experimental Studies
Table 14: Frequency of Occurrence of Failures to Respond to Alarm Annunciators in Westinghouse Human Reliability Assessment
Table 15: T/AST/058 Elements Against Westinghouse Position
Table 16: Assessment of Westinghouse Processes for Delivering Human Factors Work
Table 17: T/AST/058 Expectations Related to Concept of Operations Definition Against Westinghouse Position
Table 18: Human Factors Contribution to System Design Review
Table 19: Implementation of Human System Interface Guidelines
Table 20: Human Factors (European) Good Practice Comparison with Westinghouse Standards and Guidance
Table 21: Assessment Findings and Generic Design Assessment Issues per Work Stream
Table 22: Generic Design Assessment Supporting Documentation for Human Factors Sampled During GDA Step 4

Figures

Figure 1: Human Factors Analysis Expectations for PCSR
Figure 2: Critical Safety Function Display for Sub-criticality

Annexes

Annex 1: Assessment Findings to be Addressed During the Forward Programme for this Reactor – Human Factors – AP1000
Annex 2: GDA Issues – Human Factors – AP1000
Annex 3: Human Actions Selected for Detailed Assessment
Annex 4: Work Stream 1 - Detailed Action Assessment Proforma

Annex 5: Work Stream 1 - Summary Results of Assessment of Human Actions

Annex 6: Work Streams 1 and 3 – Recalculation of Squib Valve Maintenance Task Human Error Potential (OPR-011)

1 INTRODUCTION

1 This report presents the findings of the Human Factors (HF) assessment of the AP1000 reactor safety submissions made by Westinghouse Electric Company LLC (WEC) under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the December 2009 Pre-Construction Safety Report (PCSR) (Ref. 17) and its supporting evidentiary information derived from the Master Submission List (Ref. 19). This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document (Ref. 2) AST/001 which defines the process of assessment within the HSE Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment, together with relevant Technical Assessment Guides (TAG) (Ref. 7), which underpin the SAPs. 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 HSE's 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 RP 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 United Kingdom (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 A 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 assessment activity.

4 This is the report of my work in GDA Step 4 which was an in-depth assessment of the December 2009 PCSR (Ref. 17) [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 In addition to this report I have also produced a second document (Ref. 77), which presents the detailed results of the assessments and analyses I undertook during GDA Step 4, and data. This secondary document is provided as a supporting reference source and is targeted at HF specialist readers. It is not intended to be read in isolation and should only be read alongside this report.

6 Completion of GDA Step 4 represents the end of my planned GDA assessment on the topic of HF for the Westinghouse AP1000 reactor.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR HUMAN FACTORS

7 The assessment strategy for GDA Step 4 for the HF topic area is described in my assessment plan, which identified the scope of the assessment and the standards and criteria that would be applied (Ref. 1). This is summarised in Section 2.2 of this report.

2.1 Human Factors in Context

8 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. ND requires that a systematic analytical approach be applied to understanding the factors that affect human performance/reliability. This should produce a demonstration that the potential for human error to adversely affect nuclear safety is reduced to As Low As is Reasonably Practicable (ALARP).

2.1.1 Human Factors in the Pre-construction Safety Report

9 T/AST/051 (Ref. 7) provides general ND guidance on the purpose, scope and content of nuclear safety cases. T/AST/051 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;
- the identification of outstanding confirmatory work;
- the risk will be ALARP; and
- decommissioning will be feasible.

10 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 propose design solutions that were no longer achievable; compromising the ALARP position.

11 My expectations for the HF contribution to the PCSR stage are illustrated in Figure 1 (taken from T/AST/058 (Ref. 7)); which also includes our analysis expectations for the preliminary safety case phase. Readers are referred to T/AST/058 (Ref. 7); our TAG on Human Factors Integration (HFI) which describes our analysis expectations for the pre-commissioning, pre-operational; site wide, periodic safety review and post operational safety cases. Broadly, our expectations are that the majority of HF analysis work should be undertaken for the PCSR; such that it can influence the design and input to the risk assessment. As the design progresses, our 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-

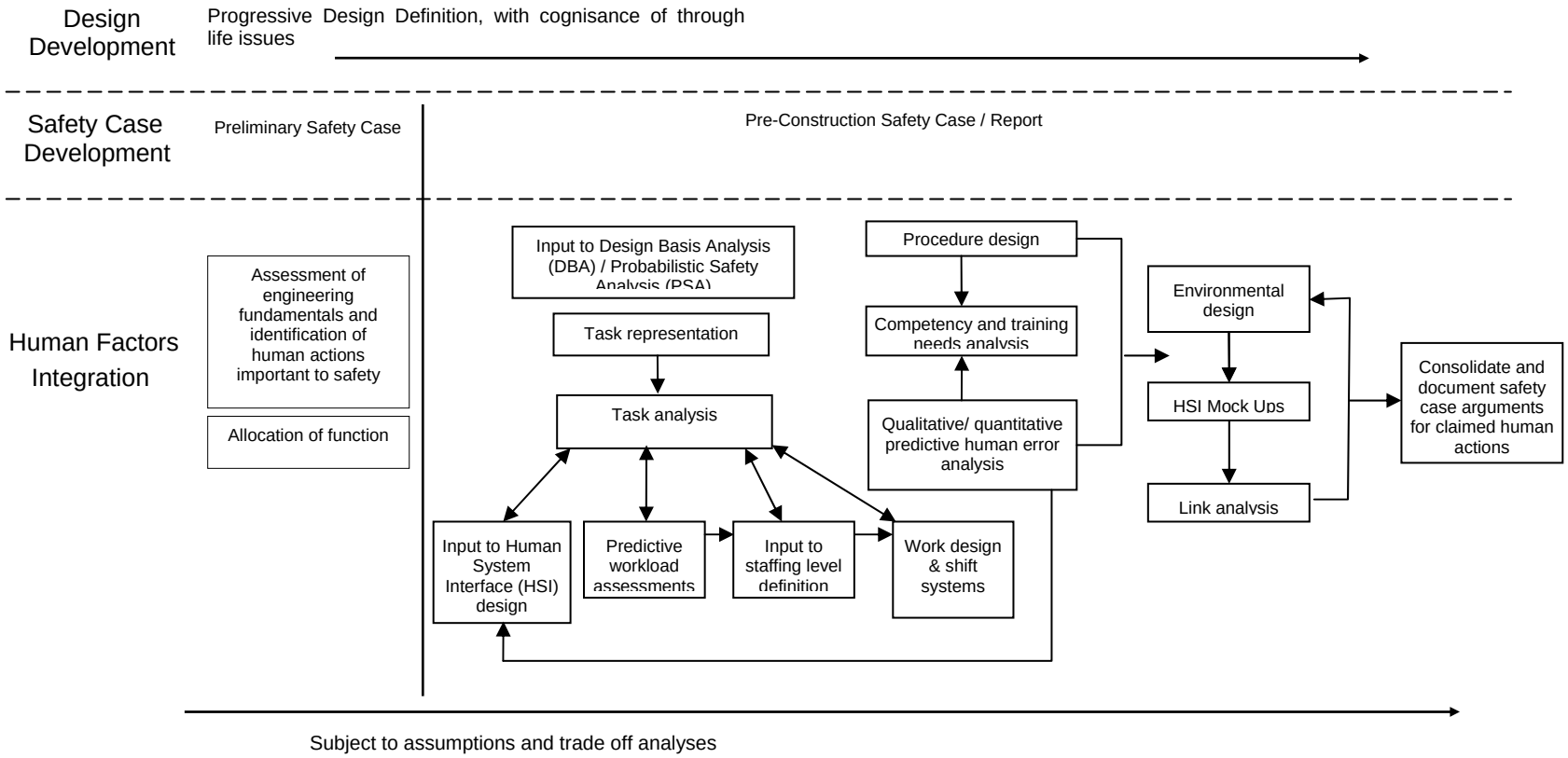
commissioning; therefore it is appropriate that the safety analysis supporting the design and operability of the proposed Nuclear Power Plant (NPP) is in place prior to the start of any (inactive) commissioning activities.

12 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 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.

2.1.1.1 Human Factors in the GDA Pre-construction Safety Report

13 An important component of the GDA PCSR is that the reactor design is submitted for ND assessment by a vendor or Requesting Party; nominally out with a potential licensee. 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 Requesting Party 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 GDA Phase 2 (site licensing) 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 PCSR



2.2 Generic Assessment Plan

14 HSE's '….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; and
- to complete a sufficiently detailed assessment to allow ND to come to a judgement as to whether a Design Acceptance Confirmation (DAC) can be issued.

15 RPs are 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; and
- arrangements for moving the safety case to an operating regime are in place.

16 Table 1 highlights the commitments provided by HSE for our GDA Step 4 assessment, and how the HF assessment makes a contribution to these commitments.

Table 1: 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 2.2.2 of this report
Judging the design against SAPs and whether the proposed design reduces risks to ALARP.	Refer to Section 2.2.5, 2.2.6, 2.2.7, 2.2.8 & 2.2.9 of this report
Inspections of the RP's procedures and records.	N/A for HF
Independent verification analyses.	Refer to Sections 2.2.5 & 2.2.6 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 2.2.6, 2.2.7 & 2.2.8 of this report
Assessing arrangements for moving the safety case to an operating regime.	Technical Query (TQ) TQ-AP1000-254 refers
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 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

Generic Step 4 Requirements	HF Consideration
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 5.2 of this report

17 My GDA Step 4 Assessment Plan for the AP1000 (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 the RP's HF processes and procedures; to give me a level of confidence in the HF analyses that I have not targeted for detailed assessment. I also focused on engineered systems that I consider novel in the UK NPP context, to ensure that an appropriate consideration has been given to HF issues in the design, to reduce the human error potential to ALARP.

18 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 2.2.5, 2.2.6, 2.2.7, 2.2.8 and 2.2.9 of this report.

19 The five work streams were nominally progressed as individual programmes of work, although there was significant cross over between particular areas; for example detail on the design of human system interfaces assessed as part of the Work Stream 5 effort was pertinent to the qualitative substantiation assessment under the Work Stream 1 programme.

2.2.1 Generic Standards and Criteria

20 SAPs (Ref. 4) have formed the basis of the HF assessment. The SAPs [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 SAPs (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.

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

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

23 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; and practice or standard more than a few years, or not subject to active on-going monitoring and review or not written by acknowledged experts may be suspect."*

24 The SAPs and TAGs employed as the main assessment basis for each of the five work streams are listed in Table 2 below:

Table 2: Safety Assessment Principles and Technical Assessment Guides used as an Assessment Basis for GDA Step 4 HF Assessments

Work Stream	Relevant HF SAPs applied	Relevant non HF SAPs applied	Relevant TAGs 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	Relevant HF SAPs applied	Relevant non HF SAPs applied	Relevant TAGs applied
Work Stream 4 – Human Factors Integration	EHF.1 EHF.2 EHF.3 EHF.4 EHF.5 EHF.6 EHF.7 EHF.8 EHF.9 EHF.10	MS.4 SC.4 SC.7	T/AST/005 – ND Guidance on the demonstration of ALARP (Ref. 7). T/AST/058 – Human Factors Integration (Ref. 7).
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).

2.2.2 Findings from Generic Design Assessment Step 3

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

Table 3: GDA Step 3 Issues Considered Further during GDA Step 4

Issue and Step 3 Report Reference	Step 4 Assessment Plan Reference
Clarity on human based safety claims, Paragraph 28	Sections 4.3.1 (4.3.5 implicit)
Accommodation of Type B Human Failure Events (HFEs) (errors leading to initiating events), Paragraph 33	Sections 4.3.1 & (4.3.5 implicit)
Selection of post fault operator actions for analysis, Paragraph 33	Sections 4.3.5 & (4.3.1 implicit)
Human Reliability Assessment (HRA) Assumptions, Paragraph 35 bullets	Section 4.3.1
Pre-initiating HFEs in shutdown faults analysis only shows post fault actions being modelled for shutdown fault sequences with no consideration of HFE contribution to shutdown initiating events, Paragraph 38 bullet 1	Sections 4.3.1 (4.3.5)

Issue and Step 3 Report Reference	Step 4 Assessment Plan Reference
Level 2 At-power Probabilistic Safety Analysis (PSA) Large Release Frequency (LRF) is sensitive to the reliability of the operator action to flood the reactor cavity post core damage, Paragraph 38, bullet 2	Section 4.3.1
Availability of documents required for assessment A set of documents are identified that are required to inform the Step 4 Assessments, Paragraph 39 bullets	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4
Non availability of HF safety case at GDA Step 3 the materials provided by Westinghouse were not an appropriate Safety Case for HF, Paragraph 40	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4
Relevance and modernity of standards and methods applied to the AP1000 design and safety case	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5
Administrative control, Paragraph 55	Section 4.3.4
HFI input to safety documentation. The application of HFI activities and expertise appears to be limited to design, not safety assessment, Paragraph 56	Section 4.3.4
Westinghouse approach to HFI, Paragraph 57	Section 4.3.4
General implications of novel technology on human reliability, Paragraph 58	Sections 4.3.1, 4.3.2, 4.3.3, 4.3.5; explicitly dealt with via Work Streams 2 and 3
Use of the Technique for Human Error Rate Prediction (THERP) for digital interfaces, Paragraph 64	Sections 4.3.1, 4.3.5 specific scope item for Work Stream 2
Scope of Human Factors Engineering (*HFE*[1]) work undertaken for AP1000 design - the scope of the programme for the AP1000 design appear focussed on control room design, Table 2 items 1, 2, 3, 4	Sections 4.3.2, 4.3.3, 4.3.4
Staffing levels for key activities, Table 2 item 11	Sections 4.3.2, 4.3.4 Explicit consideration of workload aspects in relation to allocation of function (AoF)
Wall display system safety significance, Table 2 item 12	Liaison with ND Control and Instrumentation (C&I) assessment team
Operator decision making, Table 2 item 14	Sections 4.3.1 & 4.3.5
Alarm handling. No information has been presented at GDA Step 3 on the strategy for managing and handling alarms, Table 2 item 17	Sections 4.3.1, 4.3.2
Control room design and layout, Table 2 items 18, 19	Sections 4.3.2, 4.3.4
Non Human System Interface (HSI) elements of the plant, Table 2 item 20	Section 4.3.2, 4.3.3

[1] The abbreviation for Human Factors Engineering (*HFE*) will be *italicised* to avoid confusion with Human Failure Event (HFE)

2.2.3 Additional Areas for Step 4 Human Factors Assessment

26 As my GDA Step 3 assessment focused principally on identification of the human based safety claims for the AP1000; the majority of my Step 4 scope is in addition to resolution of issues identified by my Step 3 assessment.

2.2.3.1 Consideration of Design Specific Human Factors Issues

27 The AP1000 is a 'novel' design, based on an initial design concept for the AP600 plant, and is based on a 2-loop Pressurised Water Reactor (PWR). It has several notable features that are relevant to my assessment. These are discussed below.

Incorporation of Passive Safety Features

28 The AP1000 design incorporates passive safety features to respond to plant faults. This has three principal impacts on my HF assessment:

- The extent of reliance on post-fault operator actions required for safe plant operation may result in a different set of demands compared with those typically understood for a PWR.
- The potential reliance of passive systems on operator (maintenance) activities.
- Potential vulnerability to correct functioning of passive systems from pre and post-fault operator errors. The shift to 'passive' systems potentially increases the relative importance of maintenance activities to safe plant operation.

Size of plant footprint

29 The AP1000 plant is very compact. In particular the containment building has a very small footprint. The design intent is that the plant should support short outages. This may present issues relating to access and the work environment for both local to plant operations and maintenance activities.

Use of computerised technology

30 The UK AP1000 applies advanced computerised technology, particularly in the Main Control Room (MCR), including

- computerised display technology;
- large screen display panels; and
- computerised procedures.

31 Although such technologies have been applied in overseas NPPs and in other industries, their application to the extent envisaged for the AP1000 is greater than in most UK NPPs currently in operation. There are a considerable number of HF issues relating to the use of computerised technology including (but not limited to):

- situational awareness;
- over-reliance on computerised systems;
- identification and response to failed or degraded systems;
- display ergonomics; and
- errors relating to software maintenance.

Application of novel technology in the UK NPP context

32 The squib valves that form a key part of the Automatic Depressurisation System (ADS) are considered novel in the UK NPP context. I recognise that the valves have been incorporated in non nuclear applications and within certain Boiling Water Reactor (BWR) designs, however their application to UK NPP safety systems is novel, and hence their vulnerability to human error requires understanding and assessment.

2.2.4 Research

33 The main area of research work undertaken was a commission into 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.

34 In addition I consulted the 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 own 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 Westinghouse's application of relevant good practice.

2.2.5 Work Stream 1: Substantiation[2] of Human Based Safety Actions

35 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 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';
- adequacy of the justification, or process intended to ensure, that claims are reasonable and will be achievable by the realised design; and
- recommendations on any key area of follow-on work and assessment that is required to ensure that key claims are substantiated.

36 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.

37 In addition the assessment considered the assumptions evident within the Westinghouse analyses and supporting documentation, along with the Westinghouse's approach to the demonstration of ALARP.

38 The work stream represents a vertical 'slice' through the safety submission. Actions for detailed assessment were selected on the basis of safety importance, novelty and complexity, and included maintenance type actions, routine operations (across all operating modes and encompassing the fuel route) and post fault operator requirements.

[2] 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.

In addition I explicitly considered qualitative dependency issues and the potential for operator misdiagnosis in post-fault scenarios.

39 The principal document assessed for this work stream was the AP1000 Human Factors Program and Assessment for the United Kingdom (Ref. 35). Subsequently a supplement to this report was received in April 2010 (Ref. 36) relating to the UK Probabilistic Risk Assessment[3] (PRA) update. This was then followed by specific supplementary submissions for the fire and flood PRA (Ref. 37) dated July 2010 and on low power and shutdown operations (Ref. 38) in October 2010. Other submissions were provided by Westinghouse in December 2010, which amplified their qualitative substantiation arguments and evidence. These December submissions relate to ROs raised during GDA Step 4 and the submission date was as agreed with the ONR. However the timing of these was such that I was unable to incorporate them into my detailed assessments for work stream 1 at GDA Step 4, and I only undertook an initial high level review to gain confidence in the approach. Together these submissions are referred to within this document as 'the HF safety case' (Ref. 35 is typically quoted as the primary reference).

2.2.5.1 Standards and Criteria

40 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.2, EKP.3, EKP.4, EKP.5, EHF.2, EHF.3, EHF.4, EHF.5, EHF.6, FA.7, FA.10 and NT.2 (Ref. 4). TAGs 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). Further standards and guidance employed are provided in Refs 25, 29 and 31.

2.2.5.2 Scope and Method

41 The Work Stream 1 programme had six elements:

(1) Pilot assessment of 9 human actions using three recognised HF methods and three different HF assessors.

42 A key aim of the pilot assessment was to determine a standard approach to be applied to the remainder of human actions that would be subject to detailed assessment.

43 Nine actions were assessed for the pilot study. Of these; six actions were determined by Westinghouse to contribute significantly to the predicted Core Damage Frequency (CDF) (i.e. their risk worth/importance), and three actions selected were determined by Westinghouse to have little or no contribution to the overall plant risk. Within the risk categories I also ensured that the sampled actions were split equally between those associated with potential Type A, B and C Human Failure Events (HFEs) as defined using the IAEA Error Classification (Ref. 29) and presented in Table 4.

[3] Probabilistic Risk Assessment is the equivalent term used in the United States of America for Probabilistic Safety Analysis (which can also be referred to as Probabilistic Safety Assessment); which is the term more commonly used in the UK.

Table 4: IAEA Error Classifications

Error Type	Description	Examples
A	Pre-initiators	Maintenance, test or calibration-induced failure events, that cause equipment to be unavailable when required
B	Initiating events	Actions, such as system misalignments, that, either by themselves or in combination with other equipment failures, lead to Initiating Events
C	Post-initiators	Human actions during a fault that, due to the inadequate recognition of the situation or the selection of an inappropriate strategy, tend to make it worse

44 In performing the initial nine assessments I was able to gain an insight to the Human Error Identification (HEI) methods applied by Westinghouse and reach a preliminary judgement on the general feasibility and reasonability of the quantified Human Error Probabilities (HEPs) and the ALARP method. The assessment methods I applied to the pilot phase were a combination of the Technique for Retrospective and Predictive Analysis of Cognitive Error in Air Traffic Control (TRACEr) (Ref. 24) and Rasmussen's Skills, Rules, Knowledge (SRK) (Refs 25, 26); Procedure to Review and Evaluate Dependency in Complex Technologies (PREDICT) and Barrier Analysis.

45 In general I aimed to consider the saliency of the signals to indicate the tasks that are to be performed; the nature of the task, the time available for the action to be performed; the information available to initiate, support and ensure effective task execution; the working environment; the physical capabilities required; the work design and organisation; the training and skill level assumed and the equipment design. In undertaking these preliminary assessments, I often had to rely upon best estimates of the quality of particular aspects of the system (the potential interfaces for example); where detailed evidence was not available. Table 5 presents the human actions that formed the scope of the pilot:

Table 5: Human Actions Assessed for the Pilot Assessment

Importance	Type A HFEs	Type B HFEs	Type C HFEs
'High' risk contribution	OPR-068: Mis-positioned Component Interface Module (CIM) prevents control signal from reaching an actuated component	OPR-099: Operator incorrectly executes the Core Makeup Tank (CMT) discharge valves operability test	ADF-MAN01: Operator fails to depressurise the Reactor Coolant System (RCS) to refill the Pressurizer
	OPR-174: Maintenance error results in Pressurizer (PZR) Safety Valve incorrect opening setpoint (fails to open or opens prematurely)	OPR-179: Operator erroneously causes inadvertent operation of ADS	ADN-MAN01: Operator fails to manually actuate the ADS

Importance	Type A HFEs	Type B HFEs	Type C HFEs
'Low' risk	CCN-MAN02: Inadvertent misalignment of Component Cooling System (CCS) Heat Exchanger	SGA-MAN01: Inadvertent opening of Steam Generator (SG) Power-Operated Relief Valve	RHN-MAN05: Operator fails to initiate gravity injection from In-containment Refuelling Water Storage Tank (IRWST) via Normal Residual Heat Removal System (RNS) suction line

(2) Tabulation of the human based safety claims and collation of the assumptions base underpinning the quantitative and qualitative risk assessment.

46 To assist my selection of human actions for detailed assessment, I tabulated the actions within the Westinghouse Human Action Database (HAD) to provide a simple overview of factors including their risk significance (e.g. CDF), assessed HEP, Operational Mode, and general description. This also provided a transparent presentation of Westinghouse's position regarding the human contribution to safety.

(3) Selection of actions for detailed assessment.

47 The HAD presented by Westinghouse in the HF safety case (Ref. 35) contains 250[4] actions. The Westinghouse screening of the HAD resulted in 87 actions for their 'full/proforma' assessment (65 from UKP-GW-GL-042 (Ref. 35); a further 7 from the supplementary submission UKP-GW-GL-069 (Ref. 36); 6 from the Fire/Flood PRA supplementary submission UKP-GW-GL-070 (Ref. 37); and 9 from the Low Power and Shutdown PRA supplementary submission UKP-GW-GL-071 (Ref. 38). The 'screened in' actions account for approximately one third of the total HAD.

48 The composition of the HAD is not homogeneous; it contains different error types relating to different plant systems, conditions and tasks. This prevented my sample being selected solely by determining a sample size, and then randomly selecting the actions; as this would not have selected a suitable breadth of actions. I used simple statistical methods to identify a nominal sample size and accounted for a representative breadth of action type in my final selection.

49 Assuming a normal distribution (whilst acknowledging the likely lack of such a distribution within the data), with a margin of error of 20% and a confidence level of 99%, a minimum sample size of 37 actions was identified based on the total HAD size of 250.

50 The specific actions selected considered the failure type (Type A, B, C HFEs); actions screened out by Westinghouse; actions of interest to the ND PSA team; actions of risk significance; system risk significance; action type; time available for the action; and

[4] On 30/12/2010 WEC provided ND with UKP-GW-GL-075 (Ref. 39) as a further supplement to UKP-GW-GL-042 (Ref. 35), which provides additional human actions identified as part of the fault and accident analysis work performed for the UK specific AP1000 PCSR (Refs. 17 & 18) (and those associated with UKP-GW-GL-073 (Ref. 40)). This work provides an additional 44 human actions; 4 of which are screened in for assessment using the WEC proforma method. The delivery date of UKP-GW-GL-075 (Ref 39) was such that these human actions were not considered within the work stream 1 assessments.

In addition UKP-GW-GL-073 (Ref 40) presents WEC's supplemental submission for HF regarding non core damage human errors with possible radioactive release. This was received by ND on 15/11/10. However the 6 actions analysed using the WEC proforma methodology were not presented in the supplemental report and were included in UKP-GW-GL-075 (Ref 39). These were therefore also not included in the work stream 1 detailed assessments.

Westinghouse assessments detailing multiple actions. Annex 3 presents the list of actions selected for detailed assessment. These included three actions previously assessed during the pilot study. These were reassessed using the standard approach methodology (described later). The 32 newly selected actions along with the 3 reassessed and the 6 remaining from the pilot study set provided a total sample size of 41.

51 In summary this resulted in:

- Type A: 13 actions (including 4 screened out by Westinghouse)
- Type B: 3 actions (including 2 screened out by Westinghouse)
- Type C: 19 actions (including 4 screened out by Westinghouse)

(4) Development of the Standard Assessment Methodology and Detailed Assessment of a further 35 actions.

52 A Standard Approach for the detailed assessments was developed and applied by my assessment team. This ensured completeness, comparability and standardisation between action assessments. In addition the approach ensured that the assessments were rigorous and evidence-based, to inform my judgement on the adequacy of the Westinghouse substantiation of its human based safety claims. I was specifically interested in answering the following questions:

- Has the claimed action been substantiated?
- Was the substantiation performed adequate for the claimed action and the risk associated with the claimed action?
- Are the methods that have been applied by Westinghouse appropriate to the claimed action?
- Does the Human Error Probability (HEP) represent a realistic probability based on the information reviewed?
- Does the claim appear to be ALARP?
- Does this assessment raise issues about the Westinghouse process for substantiation?
- Have Westinghouse's methods been applied in a systematic way?

53 The standard approach was informed by the pilot study, and lessons learned from that were incorporated in to the revised method. The detail of how this was undertaken is discussed in Ref. 28. The resultant standard approach contained 4 sections:

- Section 1 identified the assessment pre-requisites. It aimed to ensure that each assessor had a common level of knowledge and understanding prior to starting the assessment.
- Section 2 comprised the development and confirmation of the assessor's understanding of the claim, its significance, and the nature of the associated errors which framed their subsequent assessment.
- Section 3 comprised the detailed qualitative assessment of the substantiation against consistently applied headings, and assessment of the quantitative derivation of the HEP(s). It also included consideration of evidence of the extent to which the claim is ALARP.

- Section 4 presented conclusions and the assessor's judgement.

54 The standard approach/proforma offered guidance to those undertaking the individual assessments on the application of assessment criteria (Annex 4 refers). This included consideration of the saliency of signals, the information available, the actual (or perceived) time available for actions, the workload, the environment in which the action was to be performed, the operators' capabilities, the work design and organisation surrounding the action, the training and skills required for reliable actions, the equipment design, ALARP issues, assumptions made by Westinghouse and those made by the assessment team.

55 Re-quantification of the Westinghouse HEPs was usually undertaken where it was judged that the Westinghouse HEP could not be supported qualitatively, and the revised calculations are highlighted in Annex 4. For those actions deemed not to be substantiated by the Westinghouse analysis, I worked with fault studies and PSA colleagues to inform my judgement on their relative importance to the plant risk.

(5) Assumptions Testing/Analytical Completeness

56 Prior to the submission of The AP1000 Human Factors Programme and Assessment for the UK, only 72 human actions were identified by Westinghouse as potentially important to nuclear safety, from the PRA. The exercise undertaken to produce the Human Factors Programme and Assessment resulted in an additional 178 safety important actions being cited from the Fault Schedule (Ref. 39), highlighting that the actions modelled in the PRA was clearly incomplete. I therefore sought to establish whether the Westinghouse HEI offered in the AP1000 Human Factors Programme and Assessment was indeed now complete.

57 I undertook this high level check via recording any implicit or explicit assumption contained in the wide range of documentation reviewed to support the pilot study. 224 safety-critical, or safety-related, assumptions were identified by this process (refer to Ref. 77), and grouped on the basis of their operations, training, procedural and technical systems' implications. The purpose of recording the assumptions was to provide transparency and enable consideration of their substantiation as I progressed the detailed assessment of the individual actions.

58 It should be noted that this high level check was not explicitly documented as a stand alone piece of assessment.

59 (6) Assessment of ALARP.

60 I undertook a high level qualitative consideration of Westinghouse's treatment of ALARP with regard to HF, against our TAG on ALARP (Ref. 7).

2.2.6 Work Stream 2: Generic Human Reliability Assessment

61 Work Stream 1 aims to assess in detail the (qualitative) 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.

2.2.6.1 Standards and Criteria

62 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:*
>
> > *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."*
>
> and also that:
>
> > *"Risk assessments should directly model dependent human errors committed by a single operator or different operators."*

63 In addition the assessments considered SAPs 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).

2.2.6.2 Scope and Method

(1) Type A Human Failure Event Methodological Considerations

64 PSA colleagues provided me with an assessment of the Westinghouse method for quantifying Type A (latent) human failure events, and a calculation verification of the conversion of data sets applied in the HRA (the HEPs presented in THERP are usually interpreted as median values rather than means, however the point quantification of a PSA should use means).

(2) The relevance of extant HRA techniques (THERP) for the assessment of modern control room task environments.

65 This focused on assessment of the relevance and suitability of HEPs generated by HRA techniques that were developed in the era of hard wired control interfaces, and whose underpinning data sources relate to hard wired human system interfaces, to PSAs of contemporary control rooms that apply digital human-computer interfaces.

66 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 within the context from which the data had been gathered, and whether that data was 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 had been derived.

(3) Assessment of Level 1 and Level 2 PSAs.

67 Westinghouse has applied THERP for the HRA in both level 1 and level 2 PSAs. It is essential that the human interactions pertinent to risk have been properly identified and addressed, irrespective of the approach used. The issue then arises whether the application of the technique is appropriate for both PSAs, particularly where similar actions are claimed in both and dependence may exist between the two. As part of this aspect of my assessment I also examined Westinghouse's approach to the modelling of errors of misdiagnosis.

(4) Assessment of dependency treatment.

68 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 HFEs from the RP's HRA.

69 This component of my assessment had three elements:

(i) *Identification of current good practices for the treatment of human error dependencies.* This was undertaken via literature review to identify relevant good practice from regulatory bodies, academic research and other internationally recognised organisations.

(ii) *Assessment of* Westinghouse*'s methodology for the treatment of dependency.* The assumptions underpinning the HRA were reviewed to identify how they address the issue of dependence and whether this was in accordance with the good practice identified in the earlier phase.

70 Westinghouse used a decision tree methodology to assign levels of dependence between HFEs within a fault sequence. This approach was reviewed to assess whether it aligned with good practice as defined in the earlier phase.

(iii) *Evaluation of the application of the methodology to a sample of HFEs modelled in the PSA.* The application of the methodology for assessing human error dependence was considered both within the derivation of individual HFE HEPs and also between HFEs within important cutsets produced by the PSA.

71 All individual HFE HEP derivations presented in Chapter 30 of UKP-GL-GW-022 (Ref. 67) were reviewed to assess their consideration of human error dependency. The claims made for the HFE in relation to human error dependence were identified and the arguments relating to dependence that underpinned the HEP were evaluated along with the supporting evidence as presented by Westinghouse.

72 To assess Westinghouse's consideration of Human Error Dependence (HED) between individual HFEs, CDF cutsets were reviewed in order to identify those cutsets with multiple HFEs that contribute the most to CDF. Four cutsets from the 'at power' PSA and two cutsets form the low power/ shutdown PSA were assessed.

73 The claims made in relation to the level of dependence between the HFEs were identified. The arguments that underpin the claimed levels of dependence and their supporting evidence were then evaluated.

2.2.7 Work Stream 3: Engineering Systems

74 This work stream has two main assessment components;

- System/equipment maintenance[5] - including inspection, calibration and testing (at a strategic level - for example the general approach to 'maintenance'). Linked to Work Streams 1 and 5; and
- Consideration of novel engineering systems - for example the ADS. My focus relates to the uncertainty of the practical maintenance and operation of such systems in reality.

[5] 'Maintenance' activities include physical testing and manipulations, surveillances, monitoring and outage related activities.

75 This work stream is important to ensure claims and assumptions about the reliability of systems and components are adequately underpinned.

2.2.7.1 Standards and Criteria

76 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 SAPs 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). In addition the following TAGs 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).

2.2.7.2 Scope and Method

(1) Maintenance / Maintainability

77 My focus here was to ensure that those safety systems with the most significant risk impact had been analysed for the human error potential during maintenance activities. I also reviewed general 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 Westinghouse maintenance human error analysis, and to inform the design for maintainability of systems.

78 In light of the issues noted in section 2.2.3.1, I also considered the human factors and reliability aspects of maintenance on passive safety systems.

(2) Consideration of novel engineered systems

79 For the UK AP1000 I particularly focused on the ADS Stage 4 squib valves, on the basis that application of this technology in the NPP context is novel to the UK. I was seeking assurance that Westinghouse had fully analysed and understood the HF issues associated with their activation, including any manual maintenance requirements. I focused on the potential for violations (e.g. potential manual override of the valves), and particularly considered the (commercial) consequences of their activation. Furthermore from a maintenance perspective I sought assurance that the design of the equipment reduced the (latent) human error potential to ALARP, to support the claimed system availability.

80 A further aspect of this component of my work was consideration of software maintenance, which I consider is a more prevalent issue in this generation of reactor design.

81 In addition, I provided support to the general GDA design issue of metrication from a HF perspective.

2.2.8 Work Stream 4: Human Factors Integration

82 The focus of this work stream is on the general processes and mechanisms in place to deliver quality HF input to the design of the UK AP1000 and the safety case for the UK.

This is particularly important in the light of the UK's sampling and targeted approach to assessment. As I do 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.

2.2.8.1 Standards and Criteria

83 The principal criterion for this aspect of my assessment is 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 SAPs (EHF.2 – EHF.10) (Ref. 4) represent the totality of necessary HF consideration during the design, development and operation of a nuclear plant. Other SAPs used during the Work Stream 4 assessments were MS.4, SC.4 and SC.7 (Ref. 4). The TAGs used during the assessments were T/AST/005 – ND Guidance on the demonstration of ALARP (Ref. 7); and T/AST/058 – Human Factors Integration (Ref. 7). The standards I have employed are provided in Refs 41, 42, 43, 45 and 47.

2.2.8.2 Scope and Method

84 This aspect of my assessment had 3 aims for assessment:

- Completeness of the Human Factors Integration (HFI) programme, particularly with reference to the Westinghouse definition of 'core', 'adjunct' and 'peripheral' areas to determine the scope of HFI provided.
- Detailed probing of HFI via examining the breadth of task analysis work undertaken by Westinghouse; reviewing the Concept of Operations; and reviewing the quality of the workload analysis.
- Testing of the HFI process by reviewing the evidence of the implementation of the HFI process (for example through reviewing the flow from task analysis to user interface design, and between the *HFE* work and the HRA work; and considering the SQEP status of analysts undertaking the *HFE* and HRA work).

85 These aims were assessed largely by documentation review, although face to face meetings were also held with Westinghouse. For each of the three components a set of assessment criteria were developed that reflected appropriate good practice as defined by the scope our HFI TAG (Ref. 7) and relevant international standards and guidance. Specifically for each of the aims the assessment examined the following:

- technical quality of HFI activities, notably the major analysis and design tasks;
- management of activity related to HF;
- information flow between aspects of design, and between design and staffing;
- information flow between human aspects of risk assessment and design; and
- practical application of HF to the design.

2.2.9 Work Stream 5: Plant-Wide Generic Human Factors Assessment

86 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.

87 Work Stream 5 is not necessarily risk informed and aims to ensure that tasks are generally supported and optimised by the design. This work stream considers the central control room specifically and local to plant work areas as appropriate.

2.2.9.1 Scope, Method of Assessment and Standards and Criteria

88 Work Stream 5 is plant-wide and considers six discrete assessment areas. These six assessment areas are not necessarily a direct replication of those cited in the Assessment Plan; some areas have been grouped and three of the areas suggested by the Assessment Plan have subsequently been omitted (training needs analysis (TNA), communications and the emergency response approach), and are taken forward via an Assessment Finding (section 4.6.9 refers).

89 In terms of the assessment of training needs analysis there is no explicit Westinghouse AP1000 TNA available for assessment.

90 With regard to the proposed assessment of communications, Westinghouse advised that communication equipment is intended to be proprietary and at the time of assessment there were no specifications available for the equipment, although I assume that the appropriate HF guidance will be provided as part of the procurement documentation. In terms of the communication protocols, Westinghouse advised and ONR concur that this is a matter for a prospective licensee and is reliant upon the proposed Conduct of Operations approach. Where communications are noted to be an important contributor to the reliability of a human based safety action, my Work Stream 1 assessment has commented.

91 In terms of the emergency response approach, it transpired that that there was no generic Westinghouse material relating to this. I have considered aspects of emergency response in my Work Stream 1 and 2 assessments, but the scope advocated by my Assessment Plan is not explicitly dealt with due to a lack of available material.

92 In addition I augmented this work stream with an explicit consideration of the task analysis programme, which was not originally envisaged in the Assessment Plan. An explicit consideration of the Westinghouse task analyses was included as it underpins the other assessment work streams, and I was seeking assurance of the credibility and adequacy of the Westinghouse approach and scope.

93 The SAPs considered during the Work Stream 5 assessments were SC.4, EKP.1, EKP.4, ELO.1, ESS.3, ESS.13, ESS.14, ESS.15, ESR.1, EHF.1, EHF.2, EHF.3, EHF.4, EHF.5, EHF.6, EHF.7, EHF.8, EHF.9 and EHF.10 (Ref. 4).

(1) Allocation of Function

94 Effective Allocation of Function (AoF) should ensure that tasks are allocated between humans and systems to account for their relative strengths and limitations. Where processes are automated I seek 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 AoF should not result in an unacceptably high or low workload. For the purposes of this 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.

95 The principal criterion for this aspect of my assessment was SAP EHF.2 (Ref. 4): *"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."* In addition I have used two principal references (Refs. 20 and 21) to inform my assessment.

96 In the absence of a particular TAG on AoF at the time of writing, the functional allocation methodology proposals made by Westinghouse were assessed against accepted HF guidance on AoF (e.g. Ref. 20). The methodology proposed by Westinghouse for determining functional allocations is fully described in Ref. 113 and is an adaptation of an AoF process described in NUREG/CR3331 (Ref. 115).

97 I then tested implementation of that methodology using a sample of 6 safety-related control room based functions that could potentially be undertaken by people or automated systems. Data about the tasks required to undertake each of these sub-functions were obtained from various documents provided by Westinghouse and by walk-throughs undertaken at the Westinghouse AP1000 MCR simulator facility using a subject matter expert with operational experience.

(2) Task Analysis

98 Compliance with accepted HF standards and guidance helps to ensure that a NPP can be operated safely and effectively. However, reliable operation also requires that the plant is designed and operated in ways that support the tasks being undertaken by operators and maintainers. Therefore, it is necessary to ensure that the design is underpinned by an appropriate programme of task analysis. This requirement is emphasized in the UK SAPs for Nuclear Facilities (Ref. 4), which state as principle EHF.5 that *"Analysis should be carried out of tasks important to safety to determine demands on personnel in terms of perception, decision making and action"*. There are also other HF requirements within the SAPs that require some underlying task analysis.

99 In the absence of a particular TAG on task analysis (although I note the consideration of task analysis in the HRA TAG T/AST/063 (Ref. 7) I applied three sets of criteria to assess the Westinghouse task analysis programme. These criteria were:

- Scope of the issues considered by task analysis; the task analysis programme should:
  - i) inform interface design decisions, particularly when relatively new interface technologies are proposed;
  - ii) support the development of written procedures and other documentation to support operational and maintenance tasks;
  - iii) provide assurances that key operational and maintenance tasks can be undertaken safely and effectively;
  - iv) provide assurances that safety-critical and safety-related tasks can be successfully accomplished within prescribed timescales and, if necessary, under adverse or degraded operational conditions; and
  - v) provide the detailed underlying task data necessary to undertake qualitative error and quantitative HRAs in support of the probabilistic safety case.

- Adequacy of the task analysis processes; it will be necessary to ensure that the:
  i) methods that are used are appropriate for examining the HF issues that are being considered;
  ii) human performance data sources are appropriate and relevant;
  iii) tasks and conditions that were assessed were appropriate to address the human or systems performance issue being considered;
  iv) tasks and conditions assessed were sufficiently complete to ensure representative findings;
  v) analysts are Suitably Qualified and Experienced Persons (SQEPs) with regard to HF issues that they can interpret the data accurately and effectively; and
  vi) insights gained from the task analysis have been effectively used to substantiate or improve the design.
- Presentation of task analysis data; the task analysis report should:
  i) describe and explain the controls on any conditions that may influence the veracity or applicability of the data that were obtained (e.g. the source of subjective opinions, the source of task timings);
  ii) identify all the constituent tasks and subtasks that have been analysed;
  iii) provide sufficient information to understand what is required of an operator or maintainer in order to successfully complete each task step;
  iv) provide sufficient information to define in sufficient detail all the interface requirements to successfully undertake a task under different conditions; and
  v) provide sufficient detail to identify any conditions or factors that may impact task performance.

(3) Workstation, workplace and environmental ergonomics

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

101 The principal criterion for this aspect of my assessment was EHF.6 (Ref. 4): *"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."* Also of relevance to this aspect of my assessment were SAPs ESS.3 and ELO.1.

102 The basis of my assessment in this area was a combination of Westinghouse technical drawings, associated documentation and physical measurements in the training and development simulator. Where habitation/access was infrequent I relaxed my assessment criteria on a proportionate basis.

103 Initially, in order to ensure that workplace dimensions comply with human requirements I assessed the anthropometric data that are applied for workplace design decisions against the following criteria:

- the anthropometric data sources must be based upon measurements of a population that is reasonably representative of UK workers;
- the anthropometric data must be applied appropriately; and

- where necessary, workspace dimensions derived from anthropometric data should take account of predictable human growth trends (Secular Trends) since the measurements were taken, for the estimated lifetime of the workspace.

104 I assessed the following workstations and workplaces:

- MCR general layout;
- Distributed Control and Information System (DCIS) workstations;
- other MCR workstations;
  i) Primary Dedicated Safety Panel (PDSP)
  ii) Secondary Dedicated Safety Panel (SDSP)
  iii) Diverse Actuation System (DAS) Panel
- Remote Shutdown Workstation (RSW);
- other control rooms;
  i) primary sampling
  ii) radwaste operations
- access routes.

105 In the absence of a specific TAG in this area the high level criteria that I applied to my were::

- controls must be positioned so that they can be reached and used by the smallest workers of a justified anthropometric working population;
- forces required to operate controls and use work tools must be such that they can be used by the weakest workers of a justified anthropometric working population;
- displays and indications must be visible and legible from normal working positions;
- working positions must have sufficient space to accommodate the largest workers of a justified anthropometric working population;
- seated workplaces must provide adjustment to ensure that all personnel can work their comfortably;
- the layout of adjacent or nearby workplaces must be arranged so that it is possible to communicate between co-workers;
- access routes must provide sufficient space for the largest workers of a justified anthropometric working population to pass without risk of harm; and
- sufficient space must be provided for operators and maintainers to undertake their tasks and to use any equipment that may be necessary.

106 I have assessed the following aspects of the environmental design:

- lighting – normal and emergency provision;
- heating and ventilation – normal and emergency provisions; and
- noise.

107 Information about the proposed design in relation to environmental factors has been taken from the December 2009 PCSR (Ref. 17) and various System Specification Documents

(SSDs) as referenced. This information has been compared against the UK HF Safety Case (Ref. 35) and the AP1000 Human System Interface Design Guidelines (Ref. 105) to determine how well the design meets the guidance material.

108 In the absence of a specific TAG relating to environmental design at the time of writing I assessed Westinghouse's proposals against the following high-level criteria:

- Personnel must not be exposed to conditions within the working environment that could cause injury or risk to health.
- Where personnel must enter potentially hazardous environments, they must be provided with adequate Personal Protective Equipment (PPE).
- The exposure of personnel to potentially hazardous environments must be minimised, by limiting exposure times and task
- The environmental conditions should lie within a range that does not degrade physical, perceptual or cognitive performance.
- In the event of a complete loss of off-site electrical supplies, it must be possible to continue to operate the reactor safely and effectively for up to 72 hours and, if necessary, bring it to a safe shutdown.

(4) Control and display interfaces including alarms

109 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.

110 The principal criterion for this aspect of my assessment is EHF.7 (Ref. 4): *"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"*. Other SAPs considered are ESS.3, ESS.13, ESS.14, ESS.15 and ESR.1. TAG T/AST/059 – Human Machine Interface (Ref. 7) presents ND's expectations with regard to HMI design and I have applied these expectations to my assessment. The principal external guidelines applied are cited in Ref. 10.

111 I assessed the hardwired Protection and Safety Monitoring System (PMS) panels, the hardwired Diverse Actuation System (DAS) panel, and a sample of the soft controls and interfaces on the Distributed Control and Information System (DCIS), PMS and Wall Panel Information System (WPIS).

112 My assessment also included the associated alarm systems related to the controls and information displays used to operate and monitor the plant. The hardwired interfaces were assessed via technical drawings, and the soft interfaces via screen formats. I also reviewed the Westinghouse style guides and interface design style guides to ensure that the guidance was appropriate, consistent and comprehensive.

(5) Procedures

113 Detailed examination of this area is not appropriate until Phase 2 of the GDA process, as the specific strategy, type and format of the range of procedures will be determined by the licensee organisation. However assumptions relating to procedure type and use are made in the GDA risk assessment 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 proposals made for GDA will require re-assessment during Phase 2.

114 The principal criterion for this aspect of my assessment is EHF. 9: *"procedures should be produced to support reliable human performance during activities that could impact on safety."*

115 I have undertaken a high level assessment of a sample of the procedures provided by Westinghouse. I considered the guidance and criteria offered by T/AST/059 'Human Machine Interface' (Ref. 7) where this relates to computer based procedures but in the absence of a TAG on procedures at the time of writing and acknowledging the status of the procedural information provided, my assessment criteria in this area were as follows:

- The wording of instructions must be clear and unambiguous.
- The procedures must be presented in a way that assists users to maintain their place within the procedure and avoid missing steps or actions.
- The structure of the procedure and the typographic cues provided must assist users to navigate through the procedure and to develop and maintain an effective mental model of the tasks and their impact on the system.
- The procedures must provide diagnostic support where required.
- The procedure must provide additional support for particularly difficult tasks (e.g. additional explanation of item location information).
- The procedure must, where appropriate, provide checks for the functional success of safety-critical and safety-related actions.

(6) Staffing and Work Organisation

116 Assurance of the suitability of the staffing and work organisation will be the responsibility of a licensee organisation. Therefore detailed examination of this area is not appropriate until Phase 2 of the GDA process. However, assumptions relating to these areas are made in the GDA risk assessment and it is on this basis that I have sought some assurance on 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.

117 SAP MS.2 (Ref. 4) states *"The organisation should have the capability to secure and maintain the safety of its undertakings"* and includes a requirement to ensure that the organisational structures are appropriate, which is clarified in the following statement *"The organisation structure and baseline staffing levels should be based on appropriate organisational design principles"*. TAG T/AST/061 (Ref. 7) provides ND's expectations for staffing levels and task organisation. I have considered these expectations in my review.

2.2.10 Regulatory Interactions with Westinghouse

118 During GDA Step 4 I had numerous interactions with Westinghouse. These were via formal written communications or meetings (in person and via telephone/video conference). My overall approach to interactions with Westinghouse was one of openness and this was reciprocated by Westinghouse. I made particular effort to inform Westinghouse of my findings as they emerged, such that they could take account of them in their ongoing work; particularly where this may have improved their position for GDA Step 4.

2.2.10.1 Technical Queries and Regulatory Observations

119 Technical Queries (TQs) were the formal method for seeking clarification or further information from Westinghouse, and Regulatory Observations (ROs) were the formal method for highlighting significant findings to Westinghouse. Details of the scope and purpose of TQs and ROs are provided in Interface Protocol between HSE Nuclear Directorate / Environment Agency and Requesting Parties; JPO/003 (Ref. 75).

120 During my GDA Step 4 assessment I raised 71 TQs. Westinghouse provided me with a response to each of these during GDA Step 4.

121 I raised 4 ROs with Westinghouse during GDA Step 4. A further RO raised during GDA Step 3 (RO-AP1000-037) was carried over to GDA Step 4 as Westinghouse was unable to provide a response to it within GDA Step 3. The 5 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 (paraphrased)
RO-AP1000-037	Transparent demonstration of human based safety claims
RO-AP1000-059	Optimistic HRA claims for post fault human actions.
RO-AP1000-090	Lack of identification of human error mechanisms.
RO-AP1000-096	Lack of analysis of misdiagnosis potential.
RO-AP1000-097	Lack of analysis of violation potential.

122 Westinghouse provided a response to each of the five ROs during GDA Step 4; however the issues remain open and are taken forward via my GDA Issue and Assessment Findings.

2.2.10.2 Meetings

123 I had 15 formal meetings with Westinghouse during GDA Step 4. These were undertaken for several reasons:

- Technical discussions to clarify regulatory expectations and understanding.
- Informing Westinghouse of my assessment progress and emerging findings.
- Providing Westinghouse 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 AP1000 MCR simulator facility).

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

Table 7: Human Factors Meetings and Discussions between ND and Westinghouse During GDA Step 4

Date	Interaction
10th December 2009	Launch of GDA Step 4 with RPs

Date	Interaction
11th December 2009	Telecon to discuss the commencement of my HF assessments for GDA Step 4 and ND's expectations
15th January 2010	Telecon to discuss PSA related matters with HF involvement for HRA purposes
4th February 2010	Meeting to discuss general update and progress
19th March 2010	Telecon to discuss general update and progress
25th May 2010	Telecon to clarify TQ-AP1000-658 regarding software design and maintenance
8th June 2010	Telecon to provide early feedback on findings arising from my assessment
5th – 8th July 2010	Visit to Westinghouse Headquarters (HQ) in Cranberry Township, Pennsylvania, USA. Visit focussed on Work Stream 1 and 5 assessments with particular activity in the AP1000 MCR simulator facility
30th July 2010	Telecon to provide further feedback on findings arising from my assessment
9th September 2010	Meeting (supplemented by video conference) to provide further feedback on my assessments and for updates on the progress of Westinghouse analysis work (including responses to TQs and ROs)
14th – 16th September 2010	Visit to Westinghouse HQ in Cranberry Township, Pennsylvania, USA. Visit focussed on Work Stream 3 and 4 assessments with particular activity using the AP1000 3D Computer Aided Design (CAD) model
8th October 2010	Telecon to discuss issues arising from Work Stream 5 assessments and to seek clarification on the design of interfaces within the MCR
11th October 2010	Telecon to clarify issues regarding TQ-AP1000-1095 regarding changes to proposed operational procedures
5th November 2010	Convergence meeting. The convergence meeting was a specific GDA Step 4 event (similar meetings were 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 • Further analysis work being undertaken by Westinghouse to support GDA Step 4 and post interim DAC phase
3rd December 2010	Meeting (supplemented by Video conference) to discuss further findings from my assessments, identified since the Convergence Meeting, along with further analysis work undertaken by Westinghouse

2.2.11 Use of Technical Support Contractors

125 Technical Support Contractors (TSCs) were commissioned to undertake 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.

126 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 TSCs were involved with the HF and HRA contribution to the design of Sizewell B (SZB) NPP. All of my TSCs 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 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.

127 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.

128 My TSCs produced assessment reports which were typically analysis of Westinghouse submissions; supplemented by visits to the AP1000 simulator, and interaction with the AP1000 3-dimensional CAD model. I closely directed and monitored the TSC work via weekly telephone conferences with the TSC team leader and monthly face to face meetings with the work stream leaders. 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 TSCs.

2.2.12 Cross-cutting Topics and Integration with Other Assessment Topics

129 HF is a Cross-cutting topic; 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
Probabilistic Safety Analysis	This is the principal area of integration as 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) and specific human actions for qualitative substantiation (Work Stream 1). In addition PSA colleagues assisted my understanding of those plant systems contributing significantly to risk; to focus my maintenance assessment work (Work Stream 3). In addition I assisted the PSA risk gap analysis work by feeding in results of my Work Streams 1 and 2 assessments.
Fault studies	I worked with fault studies colleagues principally on the spent fuel pond, as significant human based safety claims were being proposed.

Assessment Area	Interaction with HF
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. Internal hazards colleagues assisted my understanding of fault initiation and progression, and the deterministic contribution of human actions in these areas.
Mechanical engineering	Squib valve maintenance was a joint focus of HF and mechanical engineering.

2.2.13 Out of Scope Items

130 The following items have been agreed with the Westinghouse as being outside the scope of GDA (Phase 1) for HF:

- detailed procedure design;
- final human machine/computer interface designs;
- work organisation;
- staffing levels; and
- administrative controls.

131 The detail of the training arrangements, work organisation (including shift system design), staffing levels and administrative control systems are decisions to be taken by the licensee organisation. Assumptions are made with regard to these aspects in the GDA risk assessment but 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.

3 WESTINGHOUSE'S SAFETY CASE

132 At the end of GDA Step 3 I concluded that Westinghouse had *"not presented a UK safety case for HF"* (Ref. 6). Early on in Step 4 (December 2009) I issued RO-AP1000-037, essentially requesting that Westinghouse develop and submit a safety case for HF. In parallel Westinghouse submitted a PCSR (Revision 2 December 2009) (Ref. 17) for assessment in GDA Step 4. I considered the HF safety arguments and concluded that the submission was not fit for purpose; there was no presentation of the claims, arguments and analytical evidence to form the basis of a HF safety case.

133 In February 2010 Westinghouse responded to RO-AP1000-037 with a safety case 'topic report' on HF (Ref. 35) (referred to throughout this document as the UK HF safety case), subsequently supplemented with additional submissions in discrete areas. The Westinghouse HF safety case consists of the base safety case report (Ref. 35) and the eight supplemental reports (Refs 36. 37, 38, 39, 40, 76, 99 and 100). It is the topic report (and the supplemental submissions) and the HRA (Ref. 67) that has formed the majority of my assessment. I should also note however that the basis of my assessment has been many hundreds of supporting documents; the most substantive of which are documented in Table 21.

134 I note that Westinghouse is committed to submitting an update to the PCSR. I briefly reviewed a draft version of the revised PCSR and concluded that it essentially proposes a direct replication of the HF topic report (Ref. 35). In addition the draft PCSR includes reference to the eight supplemental reports (Refs 36. 37, 38, 39, 40, 76, 99 and 100) and their findings, and sections have been added relating to Westinghouse's "Overarching ALARP approach" and "UK Nuclear Worker Stereotypes". I confirmed with Westinghouse via TQ-AP1000-1278 that they do not propose any fundamental change to the claims arguments and evidence for HF in the revised PCSR.

135 This section therefore summarises the principal safety proposition for HF based on the HF topic report (and supplementals) and the HRA.

3.1 Quantitative Human Reliability Assessment

136 Chapter 30 of the PRA (Ref. 67) is the presentation of the HRA. Of particular note is the citation that *"the AP1000...HRA...is the same as was provided in Chapter 30 of the AP600 PRA. There are no new operator actions modelled in the AP1000 PRA. The operator actions, available actions times and other associated assumptions made in the AP600... [HRA]... can be applied to the AP1000"*. I note that the AP600 HRA dates from c1997.

137 Chapter 30.4 (Ref. 67) documents the main assumptions that were applied to the HRA. These relate to diagnosis modelling, initiation of operator actions, dependency modelling, operator stress level, control room indication, unproceduralised control recovery, local recovery, operator actions less than and greater than five minutes, slack time, time window and actual time, omission error and dependency among cues. Of particular note are the following assertions:

- *"The Emergency Response Guidelines (ERGs) are based on symptomatic responses to an emergency operating situation and therefore reduces the diagnosis of an event to responding to cues;*
- *Visual and audible alarms serve as prompts for initial operator response, for an abnormal plant condition resulting in a reactor trip; operator activity begins with the proceduralised step in AE-0, within which diagnosis of the event is conducted.*

- *During an emergency, two operators (the Reactor Operator (RO) and Senior Reactor Operator (SRO)) are assumed to be carrying out the action in the MCR and another two operators (balance of plant and auxiliary operator) are assumed to be available to perform the actions on support systems outside of the MCR.*
- *Currently there are no established or widely accepted HEPs for using advanced digital controls and displays. The THERP nominal HEPs for conventional control room Man Machine Interfaces (MMI) were used in computing the HRA values. However the controls and displays that will be available in the AP1000 control room will be superior to the conventional control room MMI and therefore the nominal HEPs are expected to be less than those employed in the current evaluation of the AP1000.*
- *Unproceduralised recovery of human errors by the Shift Technical Advisor (STA) is applied to an event having both a time window greater than 10 minutes and a slack time. In general, unproceduralised recovery by the SRO is applied to any event having a time window greater than five minutes.*
- *Defining the estimated actual time to perform an operator action on the AP1000 is done by engineering judgement. These times are estimated…by…system designers; systems analysts, emergency procedures developers, and human reliability analysts. If the operators have more time than the average time needed to complete the task, then it is assumed that the operator's performance is not time dependent.*
- *Although emergency procedures do not have space for check off...operator talk-throughs... [indicate] that, during an emergency , the operator uses pencil checks ...to check off steps that are completed.*
- *If secondary cues are available, it is assumed that the operator can recover from an error of detection or diagnosis made when using the primary cues."*

138 There is no consolidated position of the quantitative human contribution to safety for the AP1000 in the PRA. As I highlighted at GDA Step 3, the PRA only lists (mainly) post fault actions, and the additional HF analysis work (including HEP quantifications) that Westinghouse undertook for GDA Step 4, has not been reflected in a PSA update. Therefore the summary of the human reliability contribution to the AP1000 PRA that I highlighted in my GDA Step 3 report remains. A summary of the human based safety claims included in the PRA and their risk importance is presented in Tables 50-7 and 50-8 of the PRA (Ref. 67).

139 The extant PRA does not offer any substantial arguments for the omission of Type A and B HFEs in the model.

140 The bulk of the HRA documentation is the quantification of human errors modelled in the event trees and fault trees. The performance shaping factors considered are 'assumed', and are very simple statements relating to the 'procedures' (short or long), the time window, estimated actual time, cues, stress and recovery. Very simple task decomposition is offered, usually of the order of between 3-5 steps.

141 Human error dependency is considered using the standard THERP approach, and a commission error procedure is documented, but seemingly not applied.

142 I note that there is no mention in the HRA documentation of the HF contribution to the model; reference is made to the inclusion of systems analysts, event tree analysts and HRA analysts only.

3.2 Qualitative Human Reliability Assessment and Human Factors Engineering

143 In the (quantitative) HRA, there is no reference to qualitative HF substantiation. The UK HF safety case document (Ref. 35) produced in response to RO-AP1000-037 post dates the quantitative HRA significantly, and there is no explicit link back to the quantitative HRA via a revision for example.

3.2.1 Structure and Broad Content of the Human Factors Topic Report

144 The UK HF base safety case document (Ref. 35) and its eight supplemental reports (Refs. 36, 37, 38, 39, 40, 76, 99, and 100) provide substantial documentation which aims to *"meet the requirements of a UK safety case through the demonstration of a systematic approach to the integration of human factors within the design of AP1000 systems and procedures, and to the assessment and analysis of risks arising from human actions or omissions impacting safety."*

145 Structurally, the document presents: the *"Human Factors Claims"*, the assessment methods employed to generate the report, the outcomes or results of each of the Westinghouse assessment processes, and presentation of the HF standards, guidance and operational experience that Westinghouse claim have been integrated into the design of AP1000 systems. There is a conclusions section that reiterates what Westinghouse consider are the salient points from the UK HF safety case, and a series of appendices which present the Westinghouse supporting data.

3.2.2 Safety Claims

146 The overarching claim made by Westinghouse in respect of the human contribution to the safety of the AP1000 is that *"the role of operators in ensuring nuclear safety in the AP1000 has been minimised"*. I note that there is no reference to ALARP in this statement. There is then a presentation of a hierarchy of sub-claims and sub-sub-claims, with a summary of the corresponding arguments and a reference to the report section that provides what Westinghouse consider to be the supporting evidence.

147 The sub-claims are (paraphrased):

- 1.1: Operators ensure nuclear safety through procedure execution and compliance, including verification of automated systems and manual intervention if required; and
- 1.2: Operator actions to ensure nuclear safety have been identified and assessed to ensure that the risk contribution from their erroneous execution will be ALARP.

148 Sub-claim 1.2 is supported by three further sub-sub-claims relating specifically to operator actions that induce initiation events, operator actions that degrade or prevent systems from performing their safety function and post fault operator actions that prevent the mitigation of or 'make worse' the initiating event.

149 The key PRA results are also summarised in argument 11 against sub-claim 1.2.3 relating to post fault operator actions:

- If no credit is taken for human actions in response to all faults the estimated CDF from internal initiating events at power is 1.37×10^{-5} per year.
- Taking full credit for human actions in response to initiating events (subject to the HEPs in the HRA), the estimated CDF from internal initiating events at power is $2.41 \times 10^{-7.}$ The contribution to this from sequences including human errors is $2.3 \times 10^{-8.}$

- If no credit is taken for human actions in response to faults for which the time window is less than 30 minutes, the estimated CDF from internal initiating events at power is 1.87×10^{-6}.

150 I therefore note that Westinghouse essentially claim that the HF safety case is one of safety and economic risk mitigation and ALARP. [I further note the comparison of numerical targets with current typical PWRs which typically offer a CDF of the order of 2×10^{-3} without operator actions and 3.9×10^{-5} with operator actions.]

151 I have tabulated what I consider to be the consolidated position for the human contribution to safety on the AP1000 in Ref. 77. This tabulation cites all of the human actions generated by the Westinghouse process for the development of the HF safety case and the supplemental submissions and highlights the HEPs for the human actions that were screened into their process, including those currently modelled in the extant PRA.

152 Of further note is the asserted reduction in the potential for operator induced system unavailability. A key component of the Westinghouse AP1000 design is that there is significantly less equipment to maintain; 50% fewer valves; 35% fewer pumps, 70% less cable and 80% fewer heating, ventilating and cooling units.

3.2.3 Westinghouse Methodology for Development of the Human Factors Topic Report

153 In the development of the UK HF safety case, Westinghouse recognised the incompleteness of the PRA model offered for GDA Step 4. The majority of its analysis and development work for the UK submission was therefore focused on amplifying and providing a transparent demonstration of what the human contribution to the AP1000 safety case actually is. This was undertaken by holding a series of multidisciplinary workshops that aimed to develop a comprehensive list of operator and maintainer actions, through systematic analysis of the passive safety and defence in depth systems claimed in the PSA event trees and UK fault schedule. These actions were then screened on a CDF contribution basis for further qualitative human error analysis. The qualitative 'human error analysis' of the screened in actions forms the majority of the HF submission for the UK. Westinghouse developed a 'proforma' approach for this analysis, which appears to be a simple tabular system that contains detail on (for example) the fault and scenario, reactor operation mode, system affected, 'factors 'promoting successful completion' 'human error description' and 'recovery opportunity'. I note the emphasis on factors promoting success at the apparent expense of 'factors promoting/affecting human error' (or human error identification) and the 'description' of human error at the apparent expense of 'analysis' of human error. There is also information on task timing, HEP estimation for latent maintenance errors (using the Human Error Assessment and Reduction Technique (HEART) method) and an ALARP statement for each of the actions.

154 Application of this methodology resulted in a total of 250 human actions being entered into a HAD, and 87 being screened in for detailed assessment using Westinghouse's proforma approach. I note the contrast with the 72 actions modelled in the extant PRA (68 post fault human actions and 4 human actions contributing to initiating events).

3.2.4 Human Factors Engineering

155 This is a discrete section of the UK HF safety case document providing information on the operating philosophy, the responsibilities of the proposed personnel and staffing arrangements, the application of industry guidelines and good practices and the integration of operating experience. Information is also provided on the scope and

content of the Human Factors Integration Plan (HFIP); which details the majority of the human factors engineering effort. High level information is provided on the target audience description, allocation of function, the task analysis programme, interface design, situation awareness, Verification and Validation (V&V), procedures, maintainability and training. Within each component area of the HFIP there is a description of the work undertaken, the aim of the analysis, the methods and standards applied, the scope, conclusions and any design application resulting from the analysis. Each area essentially provides summary statements of what has been done, how and why. I note that within the body of the safety case there is little information on how the human factors engineering effort has reduced the potential for human error to ALARP, and how the analysis has supports the human contribution to safety. I further note that the style of this section is similar in approach and content to the Design Control Document (DCD) chapters (Ref. 64) which I considered during GDA Step 3.

156 I acknowledge the additional analysis submitted by Westinghouse in December 2010 in response to ROs RO-AP1000-090, RO-AP1000-096 and RO-AP1000-097, and that these analyses contain a significant volume of supporting evidence for the Westinghouse HF safety case. However the timing of the delivery was such that I was not able to fully consider that material in GDA Step 4.

3.2.5 Supporting Data – Appendices

157 The majority content of the UK safety case for HF is the proforma assessments for the individual human actions. These account for approximately 80% of the submission for HF.

4 GENERIC DESIGN ASSESSMENT STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR HUMAN FACTORS

4.1 Structure of Section

158 My assessment is provided in line with the five individual work streams outlined in Sections 2.2.5, 2.2.6, 2.2.7, 2.2.8 and 2.2.9. My consolidated judgements are provided following consideration of the individual work streams.

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

159 It is clear that Westinghouse has made substantial and significant progress in the area of qualitative HF substantiation, from the end of GDA Step 3. Westinghouse has undertaken a large volume of original analysis to develop its safety case for HF in a relatively short period of time. Its approach to developing this work has been commendable, and throughout GDA Step 4 I have found Westinghouse's team to be open and willing to respond to regulatory concern and clarification, with the aim of achieving as robust a safety case as possible. As with the majority of regulatory assessment there remain outstanding items and Assessment Findings to be addressed and these are explored below. However my overall judgement is that Westinghouse has produced a PCSR submission that is largely adequate in this area.

160 In the HF safety case (Ref. 35) Westinghouse makes several specific HF claims that address the role of operators in safely operating the AP1000. The scope of Work Stream 1 is such that all of these are pertinent to this area of my assessment.

161 The overarching claim made by Westinghouse is that: *"The role of the operators in ensuring nuclear safety in the AP1000 has been minimised"* (Claim 1.0 Ref. 35).

162 Subsidiary to this further claims are made: *"The operators ensure nuclear safety throughout all plant modes of operation through proper plant procedure execution and compliance, including verification of proper automated system operation and manual intervention when needed"* (Claim 1.1 Ref. 35) and *"Operator actions required to ensure nuclear safety have been identified. Erroneous execution of these actions has been assessed to ensure the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2 Ref. 35).

163 Claim 1.1 is supported by two arguments (each provided with associated evidence):

- *"The operating philosophy of the MCR operator is to monitor and control the plant safely under normal, abnormal and emergency conditions*…….(Argument 1 Ref. 35); and
- *"It is important to the operating philosophy of the AP1000 that operator tasks are performed according to a procedure. A complete set of procedures has been developed for all plant operating modes and for activities including maintenance, normal operation, abnormal operation and emergencies……* (Argument 2 Ref. 35).

164 Claim 1.2 is supported by a further three sub-claims and nine associated arguments. Of most relevance here are the sub-claims which collectively define the scope of Westinghouse's consideration of human actions:

- *"Operator actions that induce initiating events (operator induced initiating events and maintenance induced initiating events) have been identified. These operator actions*

have been assessed to ensure the contribution to risk associated with their occurrence will be ALARP." (Claim 1.2.1 Ref. 35).

- *"Operator actions that degrade or prevent systems from performing their safety functions have been identified (i.e. maintenance latent errors). These operator actions have been assessed to ensure that the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2.2 Ref. 35).
- *"Operator actions that prevent the mitigation of or make worse the initiating event have been identified. These operator actions have been assessed to ensure that the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2.3 Ref. 35).

165 This section explores the robustness of these claims and arguments against the evidence presented. The evidence base that I have assessed the claims and arguments against is summarised in Table 21.

4.2.1 Detailed Assessment of Human Actions

166 The findings presented here relate to items (1), (2), (3) and (4) in the scope and method presented at Section 2.2.5.2. The specific findings which relate to the assessed Actions/HFEs are summarised in Annex 5. The full assessments result in 149 pages of detailed analysis; these are documented in a supplement to this report (Ref. 77) for brevity.

4.2.1.1 Overview of Findings

167 I consider that the workshop/judgement approach to deriving/identifying the additional safety relevant human actions, and the basic screening algorithm developed by Westinghouse to determine those actions requiring a more detailed assessment largely adequate; particularly in light of the incomplete and mature PSA model. It is evident that the process has produced additional insight into the human error potential, above that of the PSA. The team involved were highly experienced and from a broad technical and operational background, and the approach considered quantitative and qualitative factors. This view is also supported by my PSA colleague, who did not offer any objection to the risk screening values employed. It has however resulted in some concern regarding the ALARP position, and this is discussed in more detail later. The proforma 'method' for the Westinghouse qualitative assessments offered some insight into task viability and reliability, but omitted several key components, which I highlighted in a series of ROs.

168 There is generally an inadequate breakdown of subtasks to identify specific task requirements and associated error mechanisms (routes to human failure), and some factors likely to affect reliability have not been given adequate consideration. This was highlighted in GDA Step 4 to Westinghouse via RO-AP1000-090 (issued July 2010).

169 Westinghouse submitted a significant volume of analyses against this ROs in December 2010, as I was completing my assessment work, and as a result I did not have sufficient time to undertake a detailed assessment of the submission. However I have been able to consider the work at a very high level, and my initial judgement is that the analysis is not sufficient to fully address the RO, as there are weaknesses in both the scope and application. As a result, I have consolidated this and other outstanding ROs into a GDA Issue (GDA Issue GI-AP1000-HF-01 refers).

170 Of the 41 actions I assessed, I consider that 36 have not been substantiated, i.e. demonstrated by Westinghouse analysis to be feasible to the required level of reliability. Of those 36, 7 are judged to be largely substantiated, yet require additional evidence. Of the 36 it is judged that 15 actions are particularly safety important, and it is these actions that should be prioritised by Westinghouse. I judge that the 36 actions will require an element of re-substantiation; with the 15 more safety significant requiring a greater level of rigour. This is highlighted in tables 9 and 10 below.

> ***AF-AP1000-HF-01 -*** *The licensee shall provide additional evidence / re-substantiation of the human actions claimed within the AP1000 UK HF safety case with particular consideration of ND's qualitative assessment of 41 human actions. In addition the licensee shall consider the ND quantification of 13 human actions as part of the HRA update. This should include consideration of those assumptions ONR considers not to be currently substantiated.*

171 From a risk gap/sensitivity perspective, I have worked with PSA colleagues and recalculated the impact on the CDF of my revised calculations. Due to the incompleteness of the model I have only been able to do this for those actions included in the PSA; namely selected post fault operator actions. The impact of the individual, revised HEPs is provided in Table 11. In addition I have estimated the combined overall impact of the revised HEPs on the CDF; and this results in an 85% increase from 2.13×10^{-7} to 3.95×10^{-7}.

172 I have recalculated some of the actions assessed and these are documented in tables 9 and 10. It is clear from these tables that there are significant differences between the proposed HEPs and my assessments of the same actions.

173 There are only tenuous links between the HRA, Operational Sequence Analysis (OSA) and UK HF analysis, which is typically important to demonstrate the appropriate targeting of qualitative HF analyses, and is an explicit requirement of our HRA TAG (Ref. 7). However I consider that there are opportunities to relate analyses as the HRA is updated post GDA Step 4 and further work is undertaken by Westinghouse as a result of the site licensing.

> ***AF-AP1000-HF-02 -*** *The licensee shall consolidate the qualitative HF analysis presented for the UK HF safety case and apply it to the revision of the PSA.*

174 Furthermore I consider that there is evidence of a general quantitative over-optimism with respect to a sizeable proportion of the claims on operators, or else inadequate evidence in support of some of the claims that have been made.

> ***AF-AP1000-HF-03 -*** *The licensee shall re-quantify the HEPs in the HRA recognising my comments in this GDA assessment report relating to over optimism. Alternatively additional qualitative evidence may be presented to support the extant numerical claims.*

4.2.1.2 Severe Accidents

175 Of the 8 human actions modelled in the L2 PSA, I assessed one from a qualitative substantiation perspective as part of the Work Stream 1 assessment; CIC-MAN01 – failure to recognise the need for and failure to isolate the containment, given core damage following an accident (Ref. 77 refers). My assessment noted that at face value the claim appears to be feasible, however the current Westinghouse evidence in this regard has not adequately demonstrated task feasibility.

176 My Work Stream 2 assessment considered two further actions as part of my work on human error dependency; LPM-REC01: failure to recognise the need for post-core-uncover RCS depressurisation during small Loss of Coolant Accidents (LOCAs) or transient with loss of PRHR, and PCN-MAN01; failure to recognise the need for and failure to open Passive Containment Cooling System (PCS) water valves to drain cooling water on containment shell. Readers are referred to Section 4.3.4.2 for further detail.

177 Also under Work Stream 2, I considered the application of the THERP HRA method to the L2 PSA; readers are referred to Sections 4.3.3.1 and 4.3.3.3 for further detail.

178 Ordinarily I would also have considered the operating philosophy and procedural and training support relating specifically to the transition to a severe accident situation. Westinghouse has offered no significant material in this regard for consideration, via the UK HF safety case at GDA Step 4, although I do acknowledge that procedures and training are generally out of scope, and in the context of GDA are primarily the responsibility of a prospective licensee organisation.

179 I note that the preferred approach will be to adopt the Severe Accident Management Guidelines (SAMG) currently applied in the US; although I have not been able to assess them. I recognise Westinghouse guidance in this area (Refs 164 and 165 refer); although I have not assessed the completeness or quality of this material.

180 I will take this forward as part of routine regulatory business subsequent to the generic PCSR phase, and I will typically expect the licensee to adopt recognised good practice in this area, as defined by the IAEA in their guidance on severe accident management programme for NPPs (Ref. 166).

> ***AF-AP1000-HF-04 -*** *The licensee shall develop the operating philosophy and procedural and training support relating to severe accident management. This should specifically focus on the transition from design basis accidents to beyond design basis accidents. I expect the licensee's approaches in this area to conform to recognised good practice as defined by the IAEA.*

Table 9: Actions of Importance Judged not to have been Substantiated by Westinghouse

Actions judged not to be substantiated and of importance following review by Fault Studies	Error Type	RAW (CDF at power unless otherwise stated)	WEC derived HEP	ND derived HEP
CIB-MAN00: Operator fails to diagnose Steam Generator Tube Rupture (SGTR)	C	9.1	1.84×10^{-3}	9.31×10^{-2}
LPM-MAN01: Operator fails to recognize the need for RCS depressurisation *(during a small Loss Of Coolant Accident (LOCA) or loss of high pressure heat removal system)*	C	2.66	1.34×10^{-3}	5.41×10^{-2}
RHN-MAN01: Operator fails to align RNS	C	1.9	2.12×10^{-3}	1.7×10^{-1}
LPM-MAN05: Operator fails to recognize the need for RCS depressurisation *(during a shutdown condition with failure of the CMTs and the RNS)*	C	1.37 (relates only to shutdown)	6.83×10^{-4}	1.0×10^{-1}
HPM-MAN01: Operator fails to diagnose need for high pressure heat removal	C	1.21	5.02×10^{-4}	2.16×10^{-1}
PRN-MAN03: Operator fails to align/control Passive Residual Heat Removal (PRHR) system operation	C	1.07	8.76×10^{-4}	1.18×10^{-1}
ADF-MAN01: Operator fails to depressurise the RCS to refill the Pressurizer	C	1.01	5.00×10^{-1}	-
ZON-MAN01: Failure to start on-site standby diesel generator.	C	1	2.67×10^{-3}	$6.5 \times 10^{-1} – 8.8 \times 10^{-1}$
OPR-011: Maintenance error leads to ADS failing to vent RCS when required (Failure can be due to squib valves failing to open due to latent error, valves inappropriately left closed (stage 4), or piping is not properly vented)	A	-	6.0×10^{-5}	-
OPR-096: Maintenance error leads to failure of a PRHR air operated outlet isolation valves to open when required	A	-	6.45×10^{-5}	-
OPR-106: Maintenance error leads to failure of recirculation squib valves	A	-	6.0×10^{-5}	-
OPR-109: IRWST level instrumentation miscalibrated or made inoperable, preventing automatic transfer to sump recirculation	A	-	6.0×10^{-5}	-
OPR-127: Operator leaves CMT isolated following maintenance	A	-	4.48×10^{-6}	-
OPR-129: CMT not vented or refilled following maintenance leaving some non-condenseable	A	-	4.76×10^{-6}	-

Table 9: Actions of Importance Judged not to have been Substantiated by Westinghouse

Actions judged not to be substantiated and of importance following review by Fault Studies	Error Type	RAW (CDF at power unless otherwise stated)	WEC derived HEP	ND derived HEP
gases				
OPR-174: Maintenance error results in PZR Safety Valve incorrect opening set point (fails to open or opens prematurely)	A	-	$6.0x10^{-5}$	$1.0x10^{-2}$

Table 10: Actions of Lesser Importance Judged not to have been Substantiated by Westinghouse

Actions judged not to be substantiated and of no importance following review by Fault Studies	Error Type	RAW (CDF at power unless otherwise stated)	WEC derived HEP	ND derived HEP
CIB-MAN01: Failure to close Main Steam Isolation Valve (MSIV) on a ruptured SG	C	5.73	$1.84x10^{-3}$	-
ADN-MAN01: Operator fails to manually actuate the ADS	C	4.63	$3.02x10^{-3}$	-
REC-MANDAS: Operator fails to diagnose an event through DAS signals or perform an activity by operating DAS controls	C	2.17	$1.16x10^{-2}$ (independent) / $5.06x10^{-1}$ (dependent)	
REN-MAN02: Operator fails to initiate recirculation during LOCA	C	1.33 (relates only to shutdown)	$1.99x10^{-3}$	-
RHN-MAN05: Operator fails to initiate gravity injection from IRWST via RNS suction line	C	1.3 (relates only to shutdown)	$1.6x10^{-3}$	-
ATW-MAN03: Operator fails to manually trip the reactor through PMS in one minute	C	1.08	$5.2x10^{-2}$	$1.99x10^{-1}$
CIC-MAN01: Operator fails to isolate containment	C	1.02 (relates only to LRF)	$5.71x10^{-3}$	-

Table 10: Actions of Lesser Importance Judged not to have been Substantiated by Westinghouse

Actions judged not to be substantiated and of no importance following review by Fault Studies	Error Type	RAW (CDF at power unless otherwise stated)	WEC derived HEP	ND derived HEP
CVN-MAN03: Operator fails to start Chemical Volume Control System (CVS) Pump B	C	1.01	1.07×10^{-3}	-
REN-MAN04: Operator fails to Initiate Recirculation (LOCA and IRWST level signal failure)	C	1	4.77×10^{-3}	-
VWN-MAN01: Operator fails to align Standby Chiller (fails to recognise the need and fails to align the standby chiller during a LOCA).	C	1	5.16×10^{-3}	1.33×10^{-1}
CCN-MAN02: Inadvertent misalignment of CCS Heat Exchanger	A	-	-	-
OPA-02: Operator fails to open manual valve to sprinklers in containment (Fire PRA)	C	-	3.0×10^{-2}	7.42×10^{-2}
OPR-067: Maintenance error results in containment isolation valve stuck open	A	-	-	-
OPR-068: Mispositioned CIM prevents control signal from reaching an actuated component	A	-	-	6.0×10^{-5}
OPR-087: Maintenance error leads to damage of the containment hatch or airlock seal	A	-	-	-
OPR-099: Operator incorrectly executes the CMT discharge valves operability test	B	-	2.4×10^{-4}	-
OPR-105: Miscalibration of plant stack radiation monitor	B	-	-	-
OPR-130: Improper Latching of a Fuel Assembly	B	-	6.0×10^{-5}	1.17×10^{-2}
OPR-132: Foreign material left behind in the Core	A	-	6.0×10^{-5}	-
OPR-150: PMS division left in partial or full bypass	A	-	-	-
OPR-151: Improper restoration of CVS system alignment following maintenance	A	-	-	-

Table 11: Core Damage Frequency Impact of Revised (ND generated) Human Error Probabilities

Action	Current RAW	Fussell Vesely	Original HEP	New HEP	New CDF
CIB-MAN00	9.1	9.838×10^{-3}	1.84×10^{-3}	9.31×10^{-2}	3.17×10^{-7}
LPM-MAN01	2.66	1.716×10^{-3}	1.34×10^{-3}	5.41×10^{-2}	2.27×10^{-7}
RHN-MAN01	1.9	2.244×10^{-3}	2.12×10^{-3}	1.7×10^{-1}	2.51×10^{-7}
LPM-MAN05	1.37 (relates only to shutdown)	-	6.83×10^{-4}	1.0×10^{-1}	-
HPM-MAN01	1.21	4.787×10^{-6}	5.02×10^{-4}	2.16×10^{-1}	2.13×10^{-7}
PRN-MAN03	1.07	-	8.76×10^{-4}	1.18×10^{-1}	-
ATW-MAN03	1.08	1.527×10^{-2}	5.2×10^{-2}	1.99×10^{-1}	2.22×10^{-7}
ZON-MAN01	1	-	2.67×10^{-3}	6.5×10^{-1} – 8.8×10^{-1}	-
VWN-MAN01	1	1.916×10^{-4}	5.16×10^{-3}	1.33×10^{-1}	2.14×10^{-7}

4.2.1.3 Generic Limitations

Use of Checklists

181 For many of the HEPs that were assessed, it was assumed by the Westinghouse modellers that the operators would use checklists, completed on paper whilst they were undertaking the tasks. For a large number of the tasks that I assessed, Westinghouse assumed that these were good paper checklists, used properly, as defined in items 1 and 2 of THERP Table 20-7. However, it is apparent that the checklist function is provided by the Computerised Procedure System (CPS) (section 4.6.7 refers). In the PRA (Ref. 67) it was stated that *"…during an emergency, the operator uses pencil checks or other marking devices to check off steps that are completed"*. However, during the ND's visit to the AP1000 MCR simulator in July 2010 (refer to Section 2.2.10.2) I observed that the operators relied solely upon the computerised procedures themselves to keep track of progress and to ensure that steps were not missed. Therefore I consider that for tasks involving the use of EOPs or AOPs, it is inappropriate to model the use of well designed paper-based checklists as a means of reducing the risk of errors of omission. However, whilst Westinghouse claim that the printed procedures are available and would be marked, it appears that it considers that the main defence against errors of omission on these tasks lies in the design of the interfaces for computer-based procedures; hence I examined these interfaces in more detail in my Work Stream 5 assessments (Section 4.6.7 refers).

182 On the flowchart and the detailed displays for the computer-based procedures, the current step box is clearly marked by a prominent thick blue line and this marking stays visible until the operator either selects the 'Down' button to move to the next step, or selects another step directly by double clicking on it. However, whilst this is functionally analogous to a paper-based checklist, I consider that there are some disadvantages in comparison to a well-designed paper-based checklist. For example whilst these interfaces certainly force the operator to make a positive action to move to the next step, because this is necessary for every step or substep that is shown separately on the flowchart display, there is a strong likelihood that an operator could move between some steps without exercising due caution. For instance, an operator could move into an automatic response mode without adequately checking task completion, or could make a premature action to move to the next step. The former error is also likely in paper-based checklists that require an excessive number of check steps, though such poorly designed checklists would not satisfy the requirements for items 1 or 2 of THERP Table 20-7.

183 However, both the flowchart and the detailed displays also provide feedback if all the conditions for that step have been met by displaying a green tick. I agree that this does provide a potential way to identify a step that may have been omitted, but I consider it a relatively weak cue and one that could be misleading, as these flowcharts indicate what the automation is reporting, rather than what the operator has actually checked, and in an abnormal situation one of the operator's most important roles is to confirm whether the automated responses are reliably occurring.

184 Unfortunately, there is not currently any human reliability data for omission errors when following computerised procedures. Therefore, for comparative purposes, in the absence such data, I consider that the most relevant THERP data for such tasks are items 3 and 4 of Table 20-7. However given the uncertainty it would be appropriate to apply the THERP data conservatively (i.e. using the full Error Factor and uncertainty bounds). I suggest that this data be applied as part of the HRA revision.

AF-AP1000-HF-05 – *When revising the HRA, the licensee shall consider the human reliability data relating to omission errors when following computerised procedures. I suggest that the most relevant THERP data for such tasks are items 3 and 4 of Table 20-7 if used with the full Error Factor weighting and uncertainty bounds.*

185 For tasks that use other procedures, it may be appropriate to use items 1 and 2 of Table 20-7 to model errors of omission. However, if a particular operating utility does not provide well designed checklists for these tasks, the HEPs that have been modelled will be optimistic.

AF-AP1000-HF-06 - *The licensee shall assess the quality of checklists available (for those plant procedures that are paper based) in terms of their support to human reliability; and consider the use of items 1 and 2 of THERP Table 20-7 to model errors of omission.*

Recovery Mechanisms

186 For many of the MCR-based HEPs, Westinghouse has assumed that the Senior Reactor Operator (SRO) and the Shift Technical Advisor (STA) provide recovery from Reactor Operator (*RO*[6]) errors. This has generally been modelled by using item 3 of THERP Table 20-22, which is defined as *"one-of-a-kind checking with alert factors"*. Where recovery is only claimed for the SRO, this is claimed at 8.1×10^{-2}. However, according to the PRA (Ref. 67), where both the SRO and the STA are claimed, Westinghouse has assumed a low level of dependency between them, and the recovery for the STA is claimed at 8.1×10^{-2} and 1.0×10^{-1} is the recovery by the SRO.

187 I consider that because the SRO and the STA fulfil different roles, their impact on error recovery is also likely to be different. As modelled by Westinghouse, the SRO will be more directly responsible for checking the *RO*'s actions against the procedures, whereas, in an emergency situation, the STA should be monitoring the critical safety functions to ensure that the plant recovery is being effective. Therefore the STA should have little direct awareness of the RO's current actions, but should be able to identify inappropriate diagnoses and courses of action. In my opinion only one of these persons should be claimed as a source of recovery, according to the type of task concerned. However, whilst this will affect the modelling, the quantitative impact will be small.

188 I also consider that the use of item 3 of Table 20-22 is not appropriate. My understanding of the background to this item is that it was derived for situations where a person was directed to make a single very specific and well-defined check. Therefore, the person was cued to make this check and did not undertake it as a matter of routine. The intention was that this was to be used to assess a situation where an operator was directed to make a specific check local-to-plant of the status of a particular plant item. Therefore, I consider that other items from Table 20-22 (such as items 1 or 2) would be more appropriate for modelling recovery from operator errors, and I suggest that this data be applied as part of the HRA revision.

AF-AP1000-HF-07 - *The licensee shall reassess the human reliability data relating to checking as a recovery mechanism. I consider items 1 or 2 from THERP table 20-22 more appropriate for modelling recovery from operator errors and I suggest that this data be applied as part of the HRA revision.*

[6] To avoid confusion with Regulatory Observations the abbreviation for Reactor Operator will be italicised to *RO*.

Qualitative dependency issues and modelling

189 It appears that dependency issues were only considered by Westinghouse for those errors associated with the HRA assessments within the PRA. A dependency model built into THERP was used for this purpose, and was typically applied to moderate the predicted recovery of the STA/SRO. However for the Type A human error assessment, Westinghouse applied the HEART method, with no dependency considerations. Therefore I consider it likely that the latent error probability assessment based on long term unavailability calculations are likely to be highly optimistic. For example, Table A-3 of the HF safety case (Ref. 35) provides estimates of the potential unavailability on demand of equipment after an error, based upon different checking regimes, and for an annual test, this gives a predicted unavailability of 8.22×10^{-8} after the first check, which I consider to be optimistic. I have similar concerns for some of the other values presented in Tables A-3 and A-4.

190 In some circumstances the claimed reliabilities for the overall HEPs were particularly optimistic. This typically occurs when a high recovery level is used for a relatively high reliability task, or when two relatively high reliability tasks are ANDed together (multiplying the probabilities under the assumption of complete independence). For instance, when two HEPs that are each assessed at 2.0×10^{-3} are ANDed together, the resultant HEP is 4.0×10^{-6}. Such reliability claims can appear to be unreasonably optimistic, and in such cases it is likely that there will be some degree of dependency between the two tasks that the analyst has not been aware of.

191 Therefore, in order to avoid claims for unrealistically optimistic human reliability, it is customary to set a level known as the Human Performance Limiting Value (HPLV) (Ref. 7), such that where HEPs are calculated at a higher reliability (low probability of failure) than the HPLV, the HPLV is applied as a conservative cut-off value.

192 Any revision to the HRA should explicitly re-consider the issue of human error dependency.

> ***AF-AP1000-HF-08 -*** *The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment, which highlights the design features to mitigate dependence mechanisms.*

193 A detailed consideration of Westinghouse's treatment of quantitative dependency is discussed in Section 4.6 of this report under the scope of my Work Stream 2.

Role of the Senior Reactor Operator

194 During the visit to the AP1000 MCR simulator in Pittsburgh in July 2010 I noted that whilst executing fault scenarios the SRO read out the procedural steps of the EOP directly to the *RO*s, who then confirmed undertaking that step. I note that this is not the post fault operating regime modelled by the HRA, which assumes a level of independence and recovery potential between the *RO* and SRO, and it is also not a typical UK NPP post fault operating regime. The UK historically does not apply a 'reader' approach to the management of post fault scenarios, and I consider it reasonably foreseeable that such a regime would not be operated in a UK NPP. Although this is largely a matter for a prospective licensee organisation it should be noted that from a risk assessment perspective, the reader approach would not afford any recovery potential between the *RO* and SRO. Any revision to the HRA should model the likely post fault operating regime accurately; and explicitly model any dependency that results as a factor of the decided post fault operating philosophy.

AF-AP1000-HF-09 - *The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.*

Role of the Shift Technical Advisor

195 I understand that the HEPs of MCR-based tasks assume that there will be an STA available in the MCR within approximately five minutes of an emergency situation occurring. This seems a reasonable assumption, provided that there is an STA with an office sufficiently close and the organisational arrangements place appropriate restrictions on the movement of the STA. This person will then be responsible for monitoring the critical safety functions, making other independent checks and ensuring compliance with Technical Specifications.

196 It is not current UK practice to have an STA role, although in current UK NPPs there is the Shift Charge Engineer (SCE) role. The SCE's office is typically adjacent to the MCR and this person is nominally the emergency controller in a site incident situation. There may be a case to be made that the SCE is analogous to the STA; although in any case there is a need for the HRA to recognise and reflect the proposed staffing structure and post fault operating philosophy determined by the licensee organisation.

AF-AP1000-HF-09 *- The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.*

4.2.2 Assumptions Testing / Analytical Completeness

197 This was a peripheral and supporting piece of assessment under Work Stream 1, and as a result only a brief commentary is offered here. The work relates to the methodology and scope defined in item (5) of Section 2.2.5.2.

198 The extent of error identification achieved is greatly improved by comparison with the content of the original PRA and earlier HF submissions. The extant PRA focused entirely on post fault operator actions, and earlier HF submissions emphasised purported 'critical human actions'. However, that work has been greatly amplified by the multidisciplinary workshop approach to the generation of the HF safety case (the Westinghouse 'fault schedule process' or 'the systematic process of human error identification'); which produced an additional 178 safety relevant human actions. These actions were then explored in some detail and had the potential for further error identification.

199 However I consider that there is a degree of incompleteness with respect to the identification of human errors, in terms of how the identified additional actions have been included in the risk assessment process. Clear demonstration of fault sequences, with individual HEPs derived and placed into the fault sequence is not evident, and the rationale for some of the HEPs is sometimes unclear. There is potential however for Westinghouse to develop this further as part of the PRA/HRA update proposed for the post GDA Step 4 period; and this is what I recommend.

AF-AP1000-HF-10 *- The licensee shall include the additional HEPs identified as part of the UK HF safety case into fault sequences as part of the PSA update.*

200 The breakdown of tasks into subtasks for subsequent detailed analysis is, largely, inadequate. Also, in a number of cases; there is an inappropriate assessment of

dependency. There is some potential over-reliance on alarms and procedures for recovery and, in the UK context, reliance on recovery on the part of the STA and SRO, at both a theoretical and practical level, may be misplaced. These elements are discussed in more detail later, and have associated Assessment Findings. They do however also highlight aspects of analytical incompleteness.

201 The full list of identified assumptions is presented in Ref. 77. Of the 168 assumptions considered, I judge that a large proportion may require further exploration and additional justification. However although there appears to be a residual analytical incompleteness, I judge that proportionately it is of little consequence due to Westinghouse's ongoing development of its HF safety case. From a GDA perspective it is important that the safety case assumptions are transparent and understood by a prospective licensee, such that they are clear on the underpinning basis of the GDA risk assessment. Therefore a prospective licensee should develop, maintain and substantiate the HF assumptions as the safety case develops.

> ***AF-AP1000-HF-11*** *- The licensee shall develop, maintain and substantiate the HF assumptions as the safety case develops.*

4.2.3 ALARP Assessment

202 These findings relate to the methodology and scope defined in item (6) of Section 2.2.5.2.

203 For its assessment of ALARP, Westinghouse developed a bespoke methodology for application within the UK HF safety case (Ref. 35), which identified potential improvement options, the cost of such options, the benefits of such options and the potential for additional risk.

204 No evidence could be found within the documentation reviewed during GDA Step 4 that an effective, over-arching ALARP process had been adopted by Westinghouse, to document the optioneering associated with high-level decisions such as whether, for example, operator actions are required in certain situations or whether there is an alternative method of operating which reduces the associated risk. I note that Westinghouse provided a response to TQ-AP1000-1143 on this subject although the timing of this TQ's arrival in mid December 2010 did not allow full consideration during GDA Step 4.

205 In addition I could not find arguments and evidence relating to an overarching ALARP process or optioneering process for the up-scaling of AP600 to AP1000, although I do acknowledge the Westinghouse response to TQ-AP1000-562 stating that *"The function allocation for operator/reactor physics with respect to core axial stability is the same for both AP600 and AP1000 designs and does NOT result in any new or changed demands for operator actions between these two plants".* My reactor physics colleagues concur with this Westinghouse position.

206 In the bespoke methodology it was also apparent that the meeting of targets, including CDF, Basic Safety Level (BSL) and Basic Safety Objective (BSO), had been used as evidence that no further assessment (ALARP) would be required to be performed on errors identified in the HAD, thereby avoiding the requirement to demonstrate that risk could not be further reduced. The methods adopted for identifying improvement benefit, potential for additional risk and the ALARP decision table I consider are open to interpretation and not sufficiently comprehensive to deal with the potential risks being considered as part of the ALARP process.

207 For each of the human errors analysed by Westinghouse in a proforma, a qualitative ALARP analysis was performed against particular criteria using the method described in Section A.6 of Appendix A of the HF safety case (Ref. 35). Westinghouse's Human Factors Working Group considered each case in turn and attempted to identify potential improvements to eliminate the error or reduce its probability. These potential improvements could be additional automation (considered, in Westinghouse's judgement, to eliminate the opportunity for error), improved HF design, improved system design, amended staffing arrangements, additional training or modified procedures. The aim of each of these interventions would be to reduce the HEP, regardless of its actual value. Each potential improvement was then subjected to a screening analysis to evaluate whether the cost grossly outweighed the value of the risk improvement, taking into account the risk significance as documented in the respective proforma and any extra risk introduced by the improvement. Potential improvements that met these criteria were then subjected to the AP1000 design change control process for full evaluation to identify all reasonably practical risk reduction measures for later implementation.

208 Through the application of an algorithm to screen out lower risk activities (including all non-radiological risks) from the ALARP assessment process, I consider that Westinghouse has demonstrated an inadequate and incomplete understanding of the ALARP process. This approach also means for activities that are screened out, there will be no attempt made to minimise the residual risk.

209 The methods adopted for identifying improvement benefit, the potential for additional risk and the ALARP decision table are too simplistic to deal with the potential risks being considered as part of the ALARP process. The methods of categorising improvement cost, improvement benefit and additional risk categories are based on ambiguous criteria, which are open to interpretation by the analyst. There should be a greater level of supporting guidance to ensure that a consistent approach is adopted by all personnel involved in the ALARP process.

210 Where the residual risk is still relatively high, a greater effort should be made to reduce the risk. However, the ALARP process adopted by Westinghouse is considered too simplistic to demonstrate that a proportionate approach has been used, whereby, the higher the risk, the greater the disproportionality needed before being considered ALARP.

211 There is additional work required and arguments to be made relating to the ALARP case. I consider it most appropriate that this be taken forward by a prospective licensee. The additional arguments required will include those relating to GDA out of scope items and should also reflect the final design solutions. I note the Westinghouse response to TQ-AP1000-1143 on this area and this should be considered as part of the work required to amplify the ALARP case for HF.

> ***AF-AP1000-HF-12 -*** *The licensee shall review the Westinghouse ALARP case for HF, to develop, amplify and complete the case as part of the site specific PCSR. This development should specifically consider the optioneering of and requirements for manual/operator actions.*

4.2.4 Conclusions

212 In general I judge that Westinghouse has applied itself to the problem of HF substantiation, and has identified some sources of operator failure that were omitted by the PRA. Westinghouse has captured and incorporated some valuable Utility input, together with some potentially useful error reduction strategies and some of the claims seem reasonable

213 There are 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 AP1000 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 PCSR phase.

214 I recognise the delivery, in November and December 2010, of material that Westinghouse proposes to address my assessment observations in the areas of operator misdiagnosis, violation potential and human error mechanisms. However as I was not able to fully consider their submission in this area within GDA Step 4, I propose a GDA Issue such that I can assess the significant gaps in the safety submission that Westinghouse's new submissions claim to fill.

4.3 Work Stream 2: Generic Human Reliability Assessment - Assessment

215 At the end of GDA Step 3, both my PSA colleagues and I reported that there are significant deficiencies with the HRA aspects of the AP1000 PSA (Refs 6 and 78). My work in GDA Step 3 relating to the HRA focused on understanding the human based safety claims, and I concluded that the model had several significant deficiencies, including the lack Type A HFE modelling. I also noted in GDA Step 3 that I considered the post fault actions assessments to be potentially optimistic, and that the HRA is primarily assumptions based.

216 The assessments that I have undertaken relating to the HRA 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 the supplementary work that Westinghouse has undertaken during GDA Step 4; and this is explored below.

217 In the HF safety case (Ref. 35) Westinghouse make three claims with particular relevance to Work Stream 2. These are that:

> *"Operator actions that induce initiating events (operator induced initiating events and maintenance induced initiating events) have been identified. These operator actions have been assessed to ensure the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2.1 Ref. 35);
>
> *"Operator actions that degrade or prevent systems from performing their safety functions have been identified (i.e. maintenance latent errors). These operator actions have been assessed to ensure that the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2.2 Ref. 35); and
>
> *"Operator actions that prevent the mitigation of or make worse the initiating event have been identified. These operator actions have been assessed to ensure that the contribution to risk associated with their occurrence will be ALARP."* (Claim 1.2.3 Ref. 35).

218 Each of these claims is supported by a number of arguments. Most significant of these are arguments 10 and 11 (which are attributed to Claim 1.2.3). These present arguments that address the diversity of components within the AP1000 design that purport to limit common mode failures caused by human error; and the effect on CDF of human actions.

219 This section explores the robustness of these claims and arguments against the evidence presented.

4.3.1 Type A Human Error Modelling Method

220 These findings relate to item (1) from the methodology and scope presented in Section 2.2.6.2. This was a small and peripheral piece of assessment to support the Work Stream 2 effort; essentially involving a check on the analytical accuracy (and hence validity) of the calculations used to derive the Type A HEPs. I assessed the formulae presented in Sections A5.3 to A5.7 in the Westinghouse HF safety case (Ref. 35) and they are correct. There are statements in A5.6 and A5.7 that the calculations are slight simplifications of a more robust approach and hence lead to some conservatism. Although these are not explained further I assume that the more robust calculations take further credit for periodic checking (e.g., 12 hourly throughout a 3 month or 1 month period), which would ordinarily result in some conservatism (the degree of conservatism would be less than a factor of two, in my estimation), however I refer to my earlier assessment comment relating to a lack of dependency consideration, which may negate any conservatism (section 4.2.1.3 refers).

221 Regarding the values used by Westinghouse in developing Tables A-3 and A-4, I note that the use of the HEART value of 0.02 (HEART generic task E) for immediate checking is quite significant. THERP values for failure of checking are rather higher, being around five times greater (see items 38 to 41 of Table 30A-4 of the Westinghouse PSA submission). It is also noted that had THERP been applied for the initial error, values a little greater than 0.003 would probably have been obtained, with some variation depending on the specific details of the task.

222 I carried out a spot check on the results presented in Tables A-3 and A-4 of the Westinghouse HF submission and the cases checked were correct.

223 The formula presented in A5.8 is correct. This is the same formula as that presented in A5.7; the difference is that the probability value used for the failure of immediate detection (with instrumentation) is 0.07, compared to the value of 0.02 used in A5.7. The value of 0.07 is taken from HEART generic task NE2, which is described as *"Identification of situation requiring interpretation of alarm/indication patterns; pattern unique but no dedicated single positive features - situation infrequent but covered by bi-monthly training, appropriate responses covered in procedures if correctly identified".* THERP would suggest a higher probability of failure for this value.

224 I also briefly assessed the screening and quantification of a (random) sample of 7 type A HFEs. The 'OPR' identifiers correspond to those in the HF safety case (Ref. 35).

- OPR-009: The evaluation assumes a frequency of manipulation of 1 per year. This particular case also covers seven individual errors, by adding together only TWO evaluations. I did not look into the acceptability of this modelling in detail but it is possible that it may be optimistic (i.e., in the worst case seven rather than two individual numbers should be summed). Otherwise the calculations appear to be correct.
- OPR-010: As in the previous case a frequency of manipulation of 1 per year is assumed, and it is not known if that is a realistic value. Otherwise the calculations appear to be correct.
- OPR-011: This calculation claims visual checks of the power supply connections, detonator assembly and charges (installation) for the squib valves. These checks are claimed to have a failure probability of 2% in recovering the initial error. As explored in my assessment of this human action in Work Stream 1 (see Section 4.2 and Ref. 77) it is not clear to me that these visual checks can reasonably be claimed to have such a high reliability of detecting these failure modes.

- OPR-067. This HEP was screened out in Appendix B of the Westinghouse HF Safety case (Ref. 35) but was included in my assessments for Work Stream 1 (see Section 4.2 and Ref. 77). The latent maintenance error in this case is related to the containment isolation system. The screening rationale given was that the HF assessment only covers errors related to the CDF assessment, and large release (large radiological consequences) is outside the scope. However, from a PSA perspective, and from the perspective of the risk of radiological consequences to the public, it is noted that containment isolation is a very risk significant system, hence this screening approach would not be acceptable within the context of fault tree modelling for the Level 2 PSA.
- OPR-068. This calculation appeared to be correct although as noted in my assessment of this human action for Work Stream 1, further qualitative justification of the nature of the task would be beneficial in providing confidence in the accuracy of the calculated HEP.
- OPR-069. Verification is claimed in the calculation, but it is not clear on reading the description when this verification is performed. If the verification is not immediately after the initial human error, the "delay model" would be applied, which potentially increases the calculated HEP somewhat. In general terms, a 24 hour delay would increase the HEP by about 10%.
- OPR-129. As in other cases a once per year frequency is assumed but it isn't known if that is realistic. Also; as noted in my assessment of the human action for Work Stream 1 (see Section 4.2 and Ref. 77), other concerns are apparent relating to the calculation of the HEP, such as the adequacy of the task breakdown and the rationale for the selection of HEART generic tasks.

225 In summary the calculations relating to the Type A human error modelling are correct, and I have not identified any inherent weaknesses in the Westinghouse approach; although in considering the modelling of the Type A human errors the assumptions relating to frequencies of manipulations, and discrete weaknesses in the related qualitative substantiation; identified in my Work Stream 1 assessment should be noted (see Section 4.2 and Ref. 77). These findings are to be considered as the safety case for the AP1000 progresses, as decisions relating to maintenance regimes for example (and other aspects of the operating philosophy relating the required substantiation) are determined by the prospective licensee organisation.

> ***AF-AP1000-HF-13*** *- The licensee shall reassess the Type A human error quantifications in light of decisions relating to maintenance regimes and frequencies and revise as appropriate.*

4.3.2 Relevance of Extant Human Reliability Assessment Techniques for the Assessment of Modern Control Room Task Environments

226 This section relates to item (2) from the methodology and scope presented in Section 2.2.6.2. I note the application of the THERP methodology to the AP1000 HRA. 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 AP1000 design questions 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.

227 85 human error data points 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

228 The detail of the four experimental studies relating to holistic tasks is reported in Ref. 77, and the error probabilities associated with them reported in Table 12 below:

Table 12: Holistic Task Experimental Studies

Holistic Task	Reported Error Probability	Comment
NPP start-up with automated support	2.0×10^{-3}	Team error probability per functional interaction
Collaborative virtual team task errors	2.0×10^{-3} (derived)	Team error probability
Decisions on tabulated parameters	5.0×10^{-3}	Individual error probability
Knowledge of finite state automation	9.0×10^{-2}	Individual error probability

Implications of Holistic Data for THERP

229 The start-up task (Ref. 79) is typical and hence no diagnosis is 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.

230 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.

231 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’. Subject preparation 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 in 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 based on this study.

232 The second study (Ref. 80) 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 a level of performance for teams distributed across space and time. The character of the tasks may be similar to those undertaken when a control room team interacts with a remotely located Emergency Control Centre.

233 The third task (Ref. 81) 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 hence 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 beyond that seen in the study.

234 The fourth study (Ref. 82) 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 system automation function has been trained and its operation is frequently experienced and it receives a strong attentional focus, their knowledge and understanding of that programmatic behaviour has an error rate of 9.0×10^{-2}. However if the automation has not been trained, is not frequently experienced and suffers from a weak attentional focus then the error rate is as high as 9.0×10^{-1} (i.e. a 90% failure rate). This shows that there is an important re-AoF issue and an overall human reliability and performance issue if automated control, delivered by a computer, 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

235 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 Ref. 77. Table 13 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 studies. I have also presented summary statistics at the end of Table 13. 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 5th and 95th centile points have been obtained from the same log values of the data. The summary statistics at the end of Table 13 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 13: Object Level Task Experimental Studies

Experimental Effect	Derived Experimental Data HEP	THERP closest 'equivalent' HEP
Parallax effects of process screen parameter reading no parallax	$1.7x10^{-2}$	No direct equivalent. Table 20-11, items 1 and 2 provide the most optimistic HEPs for the check reading of displays at $1x10^{-3}$.
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 $5x10^{-4}$.
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 $5x10^{-4}$.
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 $5x10^{-4}$.
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 $5x10^{-4}$.
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

Table 13: Object Level Task Experimental Studies

Experimental Effect	Derived Experimental Data HEP	THERP closest 'equivalent' HEP
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
Diagnostic decision making performance no time pressure	$3.1x10^{-1}$	Table 20-1, item 6, $1x10^{-4}$
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	$3.0x10^{-2}$	No THERP equivalent
Virtual team collaborative error	$2.0x10^{-3}$	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 $5x10^{-4}$.
95th centile	$5.0x10^{-1}$	$1.6x10^{-2}$
Lognormal distribution mean	$2.9x10^{-2}$	$4.0x10^{-3}$
5th centile	$2.5x10^{-3}$	$2.4x10^{-4}$

236 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 Ref. 77.

237 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 is reported in Ref. 77.

238 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. I suggest that prospective licensee organisations consider the applicability of extant HRA methods to the AP1000 HRA revision; and note my regulatory expectations in this regard as cited in SAP EHF. 10 (para. 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 063 on HRA.

> ***AF-AP1000-HF-14*** *– The licensee shall consider the applicability of extant HRA methods to the AP1000 HRA revision; and note my regulatory expectations in this regard as cited in SAP EHF. 10 and TAG 063 on HRA. In the absence of justified and directly applicable HRA data, the licensee should apply a precautionary principle to assigning HEPs (e.g. the use of uncertainty bounds).*

4.3.3 Application of the THERP Method and Treatment of Diagnosis in Human Reliability Assessment

239 The two aims of this aspect of my assessment were to:

- examine the generic application of the THERP method to the HRAs that Westinghouse has presented in the Level 1 and Level 2 PSAs; and
- examine the Westinghouse treatment of diagnoses in HRA.

240 These findings relate to item (3) from the methodology and scope presented in Section 2.2.6.2.

4.3.3.1 General Application of the THERP Method

Westinghouse Modelling Content Overview

241 Westinghouse has not applied the expected THERP process, as they have not relied upon claims of diagnosis as provided in THERP Table 20-3. Westinghouse state that they expect operators to question procedures and to consider whether they are achieving the desired outcome; however their analysis does not place claims on knowledge-based diagnosis.

242 The Westinghouse HRAs for post-fault actions have a generic three-part structure :

- Activation: the phase within which the *RO* will become aware of the need to act in order to fulfil the function required.
- Corrective action: where interactions are undertaken by the *RO* with the process to manually implement the functions required for nuclear safety.
- Activation or corrective action recovery: which is conditionally required if the *RO* fails to perform either of the previous two phases. This might be by their complete omission or by errors of commission. The identification of errors of commission or omission is contingent upon Westinghouse analytical insight. Westinghouse also claim recovery potential for both activation and corrective action.

Activation Phase

243 Where a claim on activation is required, Westinghouse has, in all but three cases, directly claimed alarms, followed by a claim on corrective action with a recovery by checking. This claim on alarms entails the recognition of the existence of a particular pattern that

equates to a symptom set, which in turn is indicative of a particular deviation. For example, in Ref. 67, CCB-MAN01 or CVN-MAN03 a response is required in each case to three (unspecified) alarms. In some instances the required alarms are specified. For example in LPM-MAN02 four RCS depressurisation alarms for low pressuriser level and low pressuriser pressure are cited. I note that the alarms claimed are not those which support decision-making in Westinghouse procedure E-0; which presents modelling issues.

244 This claim on alarms is in contrast to the THERP approach to diagnosis modelling (the exceptions are REN-MAN04, RTN-MAN01 and VLN-MAN01). The Westinghouse argument for doing so is reproduced in its entirety in paragraph 308 below.

245 I note that the model does account for stress in the activation phase, although the calculation of unreliability has not been influenced by the time available to perform the task, as the THERP diagnostic table has not been used.

246 Recovery by both the SRO and the STA is assumed as a matter of course in the activation phase: thereby implicitly assuming that the *RO* makes the recognition/diagnosis of the fault. There is no modelling recognition of the dependency that will exist in this regime, which is in contrast to THERP Table 20-4, and results in the HRA assessments tending to be optimistic.

247 I have taken a random sample of the claims placed upon alarms from the tabulated results presented in the Westinghouse HRAs in Ref. 67. The frequency of occurrence for each type of claim is presented in Table 14 below, together with the corresponding HEP.

Table 14: Frequency of Occurrence of Failures to Respond to Alarm Annunciators in Westinghouse Human Reliability Assessment

WEC Item No.	Fail to respond to one of a number of annunciators alarming closely in time	HEP	Frequency of occurrence in HRA
46	One annunciator alarming	2.7×10^{-4}	6
47	Two annunciators alarming	1.6×10^{-3}	8
48	Three annunciators alarming	2.7×10^{-3}	14
49	Four annunciators alarming	5.3×10^{-3}	4
50	Five annunciators alarming	8.0×10^{-3}	6
51	Six annunciators alarming	1.3×10^{-2}	0
52	Seven to ten annunciators alarming	1.3×10^{-1}	6
53	More than ten annunciators alarming	3.6×10^{-1}	1
	Total number of claims on annunciators		**45**

248 Table 14 illustrates clearly that the majority of claims are based upon only three annunciators alarming. This is not substantiated by any evidence that Westinghouse has offered. In practice, it is more likely that post fault situations will result in a much larger number of alarms being present and a much greater probability of error in responding to

alarms. Furthermore the existence of coincident faults would result in a number of standing alarm patterns - one pattern relating to each fault.

249 When the items in Table 14 above are compared to the reliabilities indicated by contemporary literature for post fault cognitive performance, as reported in Ref. 77, it appears that the majority of the Westinghouse claims upon alarms are optimistic.

250 As part of the revision to the HRA, a prospective licensee should consider the appropriateness of sole reliance on alarms during the activation phase.

> ***AF-AP1000-HF-15*** *- The licensee shall provide detailed justification of the appropriateness of sole reliance on alarms during the activation phase.*

Corrective Action Phase

251 The Westinghouse model selects corrective actions from references in existing THERP tables, although the post fault operating regime applies computerised post fault procedures. There is therefore a question of applicability. The general issue of THERP data applicability to modern control room environments has been previously discussed in Section 4.3.2 of this report.

252 THERP makes a simplifying assumption that errors of omission arise from failures to follow the procedure whereas errors of commission arise from failures either to select the right control or display or to operate it correctly. The Westinghouse model generally includes errors of omission arising from failures to follow procedures, but the corresponding interaction with an object to alter the plant or equipment state has not always been included. Therefore some of the assessments are optimistic due to missing plant interactions. During the revision to the HRA a prospective licensee should consider relevant plant interactions, and model them appropriately.

> ***AF-AP1000-HF-16*** *- The licensee shall ensure that the revision to the HRA fully considers relevant plant interactions and models them appropriately.*

253 Examples of such missing interactions with control or display objects include, amongst others:

- LPM-MAN02 failure to read instrument(s) to verify cues is missing.
- LPM-MAN05 failure to select an (unspecified) interface device to acknowledge a cue AND failure to operate an (unspecified) interface device to acknowledge a cue are both missing.
- CCB-MAN01 failure of selection AND operation interaction(s) with Component Cooling Water (CCW) pump B interface are both missing.
- CIB-MAN00 Failure to select correct steam generator level missing AND failure to correctly read steam generator level are both missing.
- ADS-MANTEST failure to select ADS motor-operated valve control AND failure to interact with correctly with ADS motor operated valve control interface are both missing.
- RTN-MAN01 failure to select automatic shutdown control device AND failure to correctly operate automatic shutdown control device are both missing.
- REG-MAN00 failure to select correct local control AND failure to correctly operate one local control for a first regulating valve AND failure to select AND failure to correctly

read local display to establish that correct startup feedwater flow has been established, are all missing.

Application of Recovery

254 Recovery is claimed for the majority of post-fault Level 1 human reliability assessments. In most cases, this involves a claim on both the SRO and STA. Westinghouse describe the general formulation for this claim in Ref. 67, in a note appended to assessments as follows: *"Recovery is evaluated by 'item 40 in HRA data table' x 'stress level' x '0.1'; where item 40 represents recovery by STA equated to 8.1E-02, and 0.1 is recovery by SRO"*. Numerically, this amounts to a recovery factor of 4.05×10^{-2} for a chosen high stress level of 5, or 1.62×10^{-2} for a chosen moderate stress level of 2.

255 The claim of 0.1 for recovery by the SRO is explained by Westinghouse in Ref. 67 Section 30.4 item f. as follows: *"Given the current operating method, with constant feedback between reactor operator (RO) and senior reactor operator, it has been determined that the senior reactor operator could recover an error made by the reactor operator on the control board. This recovery is assigned the unconditional human error probability of 8.1E-02, described by THERP as "one-of-a-kind checking with alert factors." To account for dependency between Senior Reactor Operator and Reactor Operator, the conditional human error probability is calculated by applying the equation from THERP, Table 20-17: (1 + 19n)/20; where n = 8.1E-02. This recovery is equated to 1.27E-01, which is rounded to 1.0E-01".* This is the 'low dependency' moderator in THERP.

256 Typically the Westinghouse claims for recovery are applied both to the activation and for the corrective action steps that may be taken following activation. I consider it generally reasonable to claim the STA for the detection and failures in activation or diagnosis, however I consider it inappropriate to suggest that they will be monitoring detailed re-alignments or levels, given the nature of their role. Therefore it seems very uncertain that they will recover errors in corrective actions by the *RO*. I consider that on these grounds STA recovery should be confined to recovery in failures of activation. I have also assumed the (almost) immediate availability of the STA in the control room; which will require substantiation via management control procedures as they become available. As part of the revision to the HRA, a prospective licensee should ensure that the modelling of error recovery accurately reflects the roles of control room personnel post fault, and ensures that there are management control procedures in place to assure the availability of the STA or equivalent in the control room following an abnormal event.

> ***AF-AP1000-HF-09*** *- The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.*
>
> ***AF-AP1000-HF-17*** *- The licensee shall develop management control procedures to ensure the availability of the STA or equivalent in the control room following an abnormal event.*

257 In general it is characteristic that diagnostic or activation failures occur when the control room team share a common misconception. On this basis it is inappropriate to claim the SRO as a mechanism for activation or diagnostic recovery as they are central to, and implicated in the initial diagnosis. On the other hand, as they are monitoring the detailed actions of the *RO* it is appropriate to consider the SRO as a plausible means for recovering failed corrective action errors by the *RO*. In line with THERP Table 20-4 this recovery should be adjusted to account for dependency.

AF-AP1000-HF-09 *- The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.*

258 I consider that the baseline reliability for checking is over-optimistic and an inappropriate selection from THERP. THERP was not designed to include post fault recovery claims by means of supervision, except over the longer term. The chosen item 40 in the Westinghouse table corresponds to THERP Table 20–22 item 3. This is *"special short-term, one of a kind checking with alerting factors"*. I do not consider that this is an appropriate task description for the role of either the SRO or STA. The THERP authors describe one-of-a-kind checking as *"…when an operator is specifically requested to check something and this checking task is not part of his normal day-to-day duties. This special checking constitutes a departure from general work procedures and the checker can be expected to approach the task with a higher level of alertness and attention"*. The example used to illustrate the task is the checker establishing that an operator has restored a diesel to the automatic start standby mode after a test. In these circumstances the checker knows that a specific event has occurred. They know the particular parameters within which error might occur and the single safety function which must be fulfilled that can be compromised by that error. This kind of check contrasts with the surveillance-type checking undertaken by the STA who is checking a number of different things, not a single narrowly defined specific thing that occupies all of their attention. In my judgement the appropriate item in THERP Table 20-22 is item 8 *"checking by a reader/checker task performer in a two-man team, or checking by a second checker, routine task (no credit for more than two checkers)"*. Even so, it is questionable whether the level of attention implied by this task is entirely appropriate. However, if applied directly i.e. without dependency this provides a benefit of $5x10^{-1}$: a halving of the *RO* error rate. (This result illustrates directly why the THERP method steers analysts away from claims for checking). During the revision to the HRA, a prospective licensee should consider the appropriateness of THERP checking reliabilities to the post fault operating philosophy proposed.

AF-AP1000-HF-07 *- The licensee shall reassess the human reliability data relating to checking as a recovery mechanism. I consider items 1 or 2 from THERP table 20-22 more appropriate for modelling recovery from operator errors and I suggest that this data be applied as part of the HRA revision.*

259 Overall, I consider that the Westinghouse claims for recovery should be far more modest. I consider that claims for recovery by the STA should be confined to activation/diagnostic error, whereas claims for recovery by the SRO should be confined to a very specific subset of *RO* errors: namely control selection errors but not control operation or the currently missing procedural omission errors. As a result I consider that the claims for recovery are optimistic both as applied to activation errors and to post-fault corrective action errors.

Treatment of Slack Time and Recovery

260 Westinghouse has claimed additional benefit for recovery where there is slack time available (additional time available as a result of the fastest credible transient timescale being in excess of the time required). However in a normal distribution of task time, half of those performing the task will perform more slowly than the average task time; therefore it may be more appropriate to consider the slowest task time taken. Furthermore, the availability of additional time does not always result in additional human reliability. Factors

such as groupthink and cognitive tunnelling or confirmatory bias can cause error to persist over time. Three Mile Island and other nuclear incidents have provided practical illustrations of this phenomenon. Unfortunately, changes in working methods, procedures and interfaces do not offer demonstrably reliable defences against such collective cognitive error mechanisms. I therefore consider that additional qualitative substantiation be offered regarding the usefulness of additional / slack time to human reliability.

> ***AF-AP1000-HF-18 -*** *The licensee shall reassess the slack time that Westinghouse claim to be available and its role in human error recovery and develop additional qualitative substantiation.*

Treatment of Coincident Faults

261 Throughout the HRA each fault is considered in isolation; no cognisance has been taken of the fact that some of the assessed faults may occur concurrently. This is significant in terms of task complexity and the time available to perform a task, and therefore the potential for failure. It is entirely plausible that the time available, as dictated by transient timescales, is less than the sum total of the time that is required to perform all the tasks required to deal with coincident faults. The Westinghouse operational sequence analysis does offer timeline analysis, but it does not provide a demonstration of the feasibility of operators to respond to coincident faults within the available timeframe.

262 I recognise that multiple coincident transients are beyond the design basis and hence not expected in the DBA, and are typically screened out of the PSA (on a frequency basis). My issue relates to transient induced hazards and hazard induced transients; and I do expect some treatment of this.

263 From an initial review of the Westinghouse analysis submitted late in December 2010 relating to RO-AP1000-090 (error mechanisms), this also does not consider coincident faults. Therefore I judge that there is insufficient qualitative demonstration that the sum total of tasks required to be undertaken by control room personnel can be performed within the time available to address coincident faults of the nature described earlier. As this is a significant gap in the safety case, I have included this requirement in the GDA Issue Action list.

264 Furthermore, the additional analysis required to support the GDA Issue Actions should include consideration of compounded faults; a transient and co-incident independent loss of required safety system; and I note that this is required in the DBA.

4.3.3.2 Overall Treatment of Diagnosis (Activation) in the Level 1 Probabilistic Safety Analysis

265 In considering this issue I focused solely on the method used for the quantification of activation. THERP proposes that post-fault activation always requires diagnosis and provides tables accordingly for the quantification of crew diagnostic error probability.

266 Westinghouse in their Major Assumptions Section 30.4 a. of Ref. 67 state that *"THERP defines diagnosis as having three components, namely detection + diagnosis + decision. The THERP definition is believed to be applicable to knowledge-based responses, whereby the operators go through more thought-processes (deciphering) in order to diagnose an event. The generic procedures (Emergency Response Guidelines) are based on the philosophy of symptomatic responses to an emergency operating situation and, therefore, reduce the diagnosis of an event to responding to cues such as alarms, annunciators, and indicators (detection); thus limiting the cognitive aspects (diagnosis +*

decision). Therefore, it is advisable not to use Table 20-3 of the THERP Handbook or similar models for actions governed by symptom-based procedures in which the operators are trained; such activities are termed rule-based actions. Although the use of symptom-based procedures may not eliminate all knowledge-based behaviors by the operators, the scope of the AP1000 human reliability analysis covers only the modeling of rule-based activities. Therefore, no credit is taken for knowledge based recovery efforts."

267 Whilst it is reasonable to suppose that the use of symptom-based procedures reduces the cognitive component, or as Rasmussen would label it, *"the knowledge-based component"* (Refs 25 and 26) in the activation phase of post-fault actions relative to fault-based procedures, it cannot eliminate cognitive performance entirely. For example, it is still necessary to have the knowledge of how the procedures are to be used.

268 I recognise that there has been some simplification of the procedures relative to previous generations of PWRs. This is due to the simpler operation of the plant and rationalisation of procedural structure by monitoring and control of critical safety functions rather than the control of faults. Nevertheless, the procedures require the user to perform discriminatory tasks to decide whether or not planned process parameters have deviated, or indeed will soon have deviated enough to justify following a logical branch within a procedure.

269 In addition, procedures are a prompt to invoke operator knowledge to assist in reliable sequential task performance, not a complete substitute for it. If this were not the case, it would not require the level of investment in training and task rehearsal that is required before operators are judged competent to control a plant.

270 It is also necessary to have the knowledge of where and how the plant indications and parameters are to be read and interpreted to follow the instructions given within the procedure. If this knowledge did not exist then post-fault actions would proceed at a considerably slower pace. Furthermore, an important aspect of an operator's post fault task must be to judge the validity of the indications that are being read. This may require consultation of redundant or diverse indications. Where diverse indications are consulted, an operator's knowledge and understanding of the physical process is required in order to properly appreciate the expected physical relationship between the two instrumented parameters being scrutinised. There is also always anticipatory and response planning behaviour taking place to ensure that the procedures being exercised are and will remain relevant to the circumstances being encountered.

271 I judge that the Westinghouse assumption of an absence of any requirement for diagnosis oversimplifies the cognitive component of post-fault NPP operation and fails to recognise the continuing importance of cognition in post fault activation behaviour, notwithstanding the improved simplicity of AP1000 technology and procedures. This has resulted in inappropriate claims upon alarms in the absence of the modelling of cognitive activation behaviour, and this should be considered by a prospective licensee as part of the HRA revision.

> ***AF-AP1000-HF-19*** *- The licensee shall model cognitive activation behaviour in the HRA revision.*

272 I have however considered the suitability of the application of the THERP diagnostic error tables instead of the current Westinghouse claims on alarms, in light of current data and HRA literature, and this is presented in Ref. 77.

4.3.3.3 Overall Treatment of Diagnosis (Activation) in Level 2 Probabilistic Safety Analysis

273 The Level 2 HRAs are contained in Table 43C-1 of Attachment 43C of Ref. 67; Chapter 43 of the December 2009 PCSR (Ref. 17). I have considered the summary table of the eight operator actions for the containment event tree nodes in Attachment C of Chapter 43. Of these eight actions, six events identified are taken from the Level 1 HRAs and the two remaining assessments contain nominal screening values.

Screening Values

274 One screening value has been chosen where the HEP has been set to unity, i.e. no credit has been taken for human performance. This is a conservative approach and requires no further comment.

275 The other screening value concerns a failure to perform manual ADS operation following earlier automatic or manual actuation failure during the later phases of an SGTR. It is stated that there are "hours available" for these actions and a nominal error probability of $1.0x10^{-1}$ has been chosen. The description of operator error highlights that an automatic or manual actuation of ADS should have already been performed at an earlier point. The fact that this has not occurred implies a potential for dependency that should either be considered by the assessment or dismissed as inappropriate. Accordingly, this screening value may, or may not, be appropriate and should be subject to qualitative HF assessment.

> ***AF-AP1000-HF-20*** *- The licensee shall reconsider and justify the screening value relating to the human action of failure to perform manual ADS operation following earlier automatic or manual activation failure during the later phases of an SGTR. In particular the potential for dependency should be considered and a qualitative HF assessment will be required.*

Level 2 HRA

276 Each of the HRA identifiers in the Level 2 event tree are also used within the Level 1 PSA and were undertaken using the THERP method. This raises a generic and fundamental question of dependency between the Level 1 and three Level 2 events; if actions that are modelled as failed in Level 1 are now being claimed for Level 2, why should they now occur? It is not appropriate to simply claim the same actions with the same level of human reliability, with no consideration of dependency between the Level 1 and Level 2 PSAs, and this should be re-evaluated as part of the HRA revision.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

277 In addition, some of the assessments in the Level 1 PSA are described as ORed within the risk model with other activation or diagnostic base events. Therefore, some of these nodes are now optimistic on two counts. However, this numerical criticism is of secondary importance. All of these events require a fundamental diagnostic or recognition event to acknowledge that the scenario now constitutes a severe accident so that mitigation actions will be informed and followed accordingly. This is entirely missing from the HRAs that are presented, and should be assessed as the part of the HRA revision.

AF-AP1000-HF-21 *- The licensee shall model in the revised HRA the requirement for operators to recognise and diagnose that a scenario has moved into severe accident territory. This should be supported by a qualitative HF substantiation.*

4.3.4 Assessment of Dependency

278 These findings relate to item (4) from the methodology and scope presented in Section 2.2.6.2.

4.3.4.1 Assessment of Dependence Within Human Failure Events

279 The methodology for the treatment of dependency used in the UK AP1000 HRA is outlined in UKP-GW-GL-022 Rev 0 Chapter 30 (Ref. 67). The methodology adopted is that provided by THERP which is consistent with current good practice with respect to dependency modelling. UKP-GW-GL-022 in chapter 30 (Ref. 67), Section 30.4 provides a statement of major assumptions used to derive HEPs in the HRA. The assumptions relevant to the treatment of dependence are discussed and evaluated below.

Assumption C

280 In relation to dependency modelling, assumption C in the report states that dependency modelling is applied wherever task success requires successful completion of ORed operator actions. This is considered to be consistent with good practice. The report then identifies that where a series of operator actions is required it is assumed that:

- *A low dependency relationship will exist between the first and second operator steps.*
- *A medium dependency relationship will exist between the first and third operator steps.*
- *A high dependency relationship will exist between the first and fourth (and any further subsequent operator steps) that exist in the ORed success sequence.*

281 A caveat to this assumption is provided such that if the analyst does not believe that the above dependency relationship exists then moderate dependency should be applied throughout the sequence.

282 The assumption as outlined above appears to run contrary to the methodology described in the THERP handbook where assessment of the level of dependence is recommended to be made between successive tasks. For example in a four step operator task, the level of dependence between task A and task B would be assessed and a conditional error probability for task B based on this derived. Next an assessment of dependence between tasks B and C would be assessed and finally an assessment of dependence between tasks C and D would be undertaken. This contrasts with the approach described in the assumption outlined above where each assessment of dependence is taken between task A and each of the remaining sub tasks comprising the overall task. The THERP handbook (Ref. 13) in chapter 10, page 10.14 states that *"In the case of an analysis involving more than two tasks, the conditional probabilities of subsequent limbs (in the HRA event tree) are derived by attributing all the effects of dependence to the immediately preceding limb"*. It is of further concern that assessment of dependence is based on assumed dependence relations between tasks. I would have expected that an explicit qualitative assessment of dependence was conducted wherever ORed operator actions were required for task success. This qualitative assessment should consider explicitly the coupling mechanisms that might affect the dependency relationship between the two tasks

283 I judge that the assessment of dependence relations as expressed in Assumption C of UKP-GW-GL-022 Chapter 30 (Ref. 67) is not consistent with the approach presented within THERP for the assessment of dependence between subsequent tasks. This should be addressed as part of the HRA revision.

284 The use of assumptions to model dependence rather than undertaking an explicit assessment of dependence relations is not considered to be consistent with HRA good practice and regulatory requirements (TAG T/AST/061 refers (Ref. 7)); and this should be addressed as part of the HRA revision.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

Assumption F

285 Assumption F in the HRA methodology provides discussion of between-person dependence effects during emergency conditions. This considers unproceduralised recovery which is argued to be provided by the SRO constantly checking the actions of the *RO* via the feedback mechanism provided by the pattern of interaction between these two operators. HEPs for failure of recovery are derived by assigning an HEP for failure of the recovery (checking) task and then assigning a level of dependence between the *RO*s actions and the checking function provided by the SRO. The assumption made is that the form of checking is best expressed by THERP as *"one-of-a-kind checking with alert factors"* (THERP table 20-19, item 3) and that this is modified by application of the low dependence equation from the THERP dependence model. The use of low dependence between the *RO* and SRO contradicts the assigned dependence levels provided in THERP, table 20-4 (number of *RO*s and advisors available to cope with an abnormal event and their related levels of dependence) which identifies the level of dependence between the *RO* and SRO as high. I have addressed this issue earlier in Section 4.3.3.1 of this report.

286 Assumption F also discusses unproceduralised recovery provided by the STA. Again the assumption made is that the form of checking is best expressed by THERP as *"one-of-a-kind checking with alert factors"* (THERP table 20-19 item 3) but again this is not well justified. A zero level of dependence between the checking function provided by the shift technical advisor and the actions of the operating crew is assumed. This contradicts the assigned dependence levels provided in THERP, table 20-4 (Number of reactor operators and advisors available to cope with an abnormal event and their related levels of dependence) which identifies the level of dependence between the STA and others as low-moderate for diagnosis and high-to-complete for detailed operations, i.e. manual actions.

287 I judge that assumption F will result in the production of overly optimistic HEPs and that this will have an effect throughout the HRA as credit is taken for unproceduralised recovery in almost all HEP derivations.

Assumption G

288 Assumption G relates to local recovery; where recovery is provided by a second operator monitoring the performance of an initial operator. THERP Table 20-19 item 1 is applied for such recovery. The mean HEP of $1.6x10^{-1}$ is applied without any further modification for the effects of dependence. This is considered to be consistent with the methodology

for the application of THERP and hence good practice in relation to the treatment of dependence, as Table 20-19 HEPs account for between-person dependence under normal operating conditions. However under abnormal operating conditions or in emergency situations no credit should be given for additional personnel as outlined in THERP Chapter 18 (Ref. 13).

289 I judge that Assumption G is appropriate for considering normal operating conditions, however for emergency or abnormal conditions this is likely to result in optimistic HEPs.

Assumption J

290 Assumption J relates to the amount of time available for recovery, when this is greater than 1 hour. In such cases credit is claimed for recovery of an operator error by another operator by applying THERP Table 20-19 item 3, adjusted for moderate dependency for at power events, and high dependency for actions performed during shutdown. It is not clear to me that the selection of the original HEP is appropriate in this instance.

291 As discussed earlier I do not consider that Westinghouse has made the case for one-of-a-kind checking, and that alerting factors are present. I consider that a more appropriate treatment for an operator detecting an error made by another within a control room, assuming the error is unannunciated but indicated by a deviant display, is provided by the display scanning model provided within chapter 11 of THERP. This should be (re)considered as part of the HRA update.

> ***AF-AP1000-HF-07*** *- The licensee shall reassess the human reliability data relating to checking as a recovery mechanism. I consider items 1 or 2 from THERP table 20-22 more appropriate for modelling recovery from operator errors and I suggest that this data be applied as part of the HRA revision.*

Assumption L

292 Assumption L in the UK AP1000 HRA relates to dependency between cues available to detect the need for action or diagnose an event. Where secondary cues are available to an operator to recover from failure to detect or diagnose an event, it is assumed that a moderate dependency will exist between the primary and secondary cues such that detection or diagnosis based on secondary cues is less reliable than that based on primary cues. Whilst this logic is correct, I would expect a consideration of the nature of the cues, their location on the display, and the time between the annunciation of primary and secondary cues to be assessed wherever a claim is made on secondary cues, as the level of dependence may be higher than that accounted for by the use of moderate dependence.

293 The assumption of moderate dependence between primary and secondary cues within an HFE may result in overly optimistic HEPs for the event. It is necessary that a detailed qualitative assessment of the dependency coupling mechanisms is performed wherever multiple cues are claimed in the HRA.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

4.3.4.2 Treatment of dependence in individual Human Reliability Assessment Event Trees

294 I reviewed the HEP derivations for individual HFEs and examined treatment of dependence within these; and this is reported below:

Assessment of Recovery Factors

295 Two different approaches were noted for the treatment of recovery factors. In instances where recovery factors were provided by both the SRO and the STA, the HEPs for failure of each of the recovery factors were multiplied together and then further modified to take into account the effect of stress, producing an overall recovery factor of 4.05×10^{-2}. Yet, when only one recovery factor was present e.g. SRO, no adjustment to the recovery HEP was applied to account for the effects of stress.

296 There appears to be no justification within the documentation for the differential application of modifiers for stress applied to recovery situations where only the SRO as opposed to the SRO and STA are present. This should be re-evaluated as part of the HRA revision.

> ***AF-AP1000-HF-22*** *- The licensee shall justify the stress modifiers applied to recovery situations as part of the update to the HRA.*

Human Failure Event LPM-MAN-05

297 This failure event describes failure to recognise the need for RCS depressurisation during a shutdown condition with failure of the core make-up tanks and the RNS system. Failure of two sub tasks (omit step to acknowledge primary cue AND omit step to acknowledge secondary cue) is required to occur for the failure to recognise the need for RCS depressurisation to occur. In the derivation of the HEP for this event, moderate dependency between these two sub tasks is claimed, but there is no evidence or justification provided for this level of dependence other than the use of assumption L discussed earlier. This should be further substantiated using evidence of the time between occurrence of the cues, the location of the display in which the cues are provided, the form of the cue, etc., otherwise it can be considered that the level of dependence assigned is overly optimistic.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

Human Failure Event LPM-REC01

298 LPM-REC01 failure to recognise the need for RCS depressurisation during a small LOCA or transient with loss of the passive residual heat removal system, and successful operation of the core make-up tanks after core damage. This event is identified as having a dependency on LPM-MAN01; an initial failure to recognise the need for RCS depressurisation in response to the LOCA or transient. A claim for low dependency is made, but there is little substantiation for this other than a claim to engineering judgement and the fact that the two events are separated by a (undefined) very long period in time. Again qualitative substantiation is required to support the low dependency assignment; it could be argued that if the need for depressurisation has not been recognised initially there is a high likelihood that the need for depressurisation will not be recognised subsequently due to operator mindset. I would expect to see some discussion of the

factors that preclude complete dependency being assigned to what is essentially the same diagnosis at two different periods in time, otherwise it cannot be demonstrated that the HEP assigned to LPM-REC01 is sufficiently conservative and that the Large Early Release Frequency (LERF) is not underestimated.

AF-AP1000-HF-23 *- The licensee shall provide additional qualitative evidence relating to dependency factors associated with human failure event LPM-REC01.*

Human Failure Event ADN-MAN01

299 ADN-MAN01 evaluates the probability of failure to actuate the ADS for RCS depressurisation as recovery from failure of automatic actuation or for manual ADS actuation. As part of this task an operator is required to actuate at least two of four stage lines by pressing two pushbuttons for each stage. At each stage complete dependency is assigned between the actions of pushing the pushbuttons. Between each stage, however, moderate dependency is claimed for failure to push the pushbuttons. There is no argument or evidence provided for why moderate dependency is appropriate and again I would expect to see some discussion of the qualitative factors that might affect dependency; location of pushbuttons, time between requirement to operate each stage, etc.

300 A further assessment of dependency is made between action ADN-MAN01 and operator action CMN-MAN01 to actuate core make up tanks; where it is claimed that ADN-MAN01 has a high dependency on CMN-MAN01. It is not clear on what basis this level of dependence is assigned, reference is made to dependency evaluation criteria, but these have not been outlined, therefore it is difficult to evaluate the appropriateness of the claim.

AF-AP1000-HF-24 *- The licensee shall reassess the level of dependency assigned between actions ADN-MAN01 and CMN-MAN01 as part of the HRA update.*

Human Failure Event ADF-MAN01

301 ADF-MAN01 evaluates the probability of failure to depressurise the reactor coolant system to refill the Pressuriser using the first stage ADS valves. In this scenario, a SGTR has occurred and depressurisation with auxiliary spray has failed; as an alternative way to depressurise the RCS, the operator is required to use one set of ADS first stage valves. This event is identified as being dependent on CVN-MAN00; human action required to manually operate the auxiliary spray system. A high level of dependency is assessed between these events, but again, no justification is provided by way of a qualitative assessment of factors that are known to affect dependence between human actions. Thus it is difficult to assess the accuracy of this claim.

AF-AP1000-HF-25 *- The licensee shall provide additional qualitative evidence relating to dependency factors associated with HFEs ADF-MAN01 and CVN-MAN00.*

Human Failure Event PCN-MAN01

302 PCN-MAN01 assesses the likelihood that an operator will fail to recognise the need for and fail to actuate the PCS air-operated valves (AOVs) if automatic actuation fails, given a transient or loss of offsite power. Within this human error event, two AND gates are present; one relates to selection of control, and the second to operation of the control, and at both gates moderate dependency is claimed between the actions. No evidence is provided for the allocation of moderate dependency between these errors. I would expect

some evaluation of the controls and the time period between the dependent actions in order to substantiate the claim. If, as I expect, the actions are performed close in time on controls located on the same panel, then the assignment of moderate dependency may be overly optimistic and high or complete dependence be more appropriate.

> ***AF-AP1000-HF-26*** *- The licensee shall reassess the dependency level assigned to HFE PCN-MAN01 as part of the HRA update.*

Human Failure Event CIB-MAN01

303 CIB-MAN01 evaluates the probability of failure to isolate the faulted steam generator following a SGTR event. Within the HFE there are 4 subtasks within which moderate dependency is assigned, where an operator is required to select or operate two controls to open or close valves. In each case it appears that both actions need to be completed for task success to be achieved (e.g. sub-task 3 Select wrong control for two of two valves on blowdown line (moderate dependency)), and therefore it seems to be inappropriate that HEPs for each action are multiplied together. The HEP for the action should be multiplied by 2 to reflect the fact that two actions have to be performed correctly. This appears to be an error in modelling the event rather than an error in the identification of the level of dependence, i.e. an OR path to success is claimed when in fact AND logic should be applied.

> ***AF-AP1000-HF-27*** *- The licensee shall reassess the modelling associated with HFE CIB-MAN01 as part of the HRA update.*

4.3.4.3 Treatment of Dependence Within Accident Sequences

Dependency Level Evaluation Decision Tree

304 As well as accounting for dependency within human error events, the UK AP1000 HRA deals with dependence between human error events within individual accident sequences, where these contain more than a single human error event. The Westinghouse assessment of dependence between individual human error events is based on consideration of four factors, these are the:

- level of stress applicable to the operator action;
- timing mechanism of the operator actions;
- complexity of the operator actions; and
- quality of the procedural guidance given to operators.

305 These factors are combined in a decision tree in order to assign a level of dependence between an initial HFE and subsequent failure events.

306 The decision tree first evaluates level of stress associated with the first human error event at three levels; low, moderate or high. The level of stress assigned appears to be a function of the nature of the event the operator is attempting to deal with. Appendix A.6 of chapter 30 (Ref. 67) indicates that levels of stress are adopted for the procedural action assessment is as follows:

- LOCAs, loss-of-offsite power, and Anticipated Transient Without Scram (ATWS): SEF = 5 (extremely high stress level and step-by-step tasks).

- Transients: SEF = 2 (moderately high stress level and step-by-step tasks).
- Normal operation: SEF = 1 (low stress level).

307 Although it is not stated, it is reasonable to assume that the same formulation is used to assign levels of stress at the first step of the dependency assessment. In practice, a review of Table 30-3 (Ref. 67) dependency level evaluation summary reveals that for the majority of dependency evaluations conducted, high stress is assigned to the first task.

308 The second factor considered in assigning dependency levels is time. Two factors are considered in relation to the second task to be performed, these are:

- The time window available for the second task, considered at 4 levels: <15mins; >15mins <30mins; >30mins <60mins; and >60mins.
- The available slack time for the second task, (available time minus required time) to complete the operator task. This is assessed at two or three levels depending on the total time available.

309 Analysis of time in this way is appropriate for assessing the independent HEP for the second task, but is not what is required to make an assessment of dependency. For dependency assessment, the important factor is not the time available, but the time between the two required actions, as applied for example in Standard Plant Analysis Risk HRA (SPAR-H) (Ref. 83) and DEPEND HRA (Ref. 84). For this reason I consider the treatment of time in the dependency evaluations to be misconceived and therefore the dependency evaluations to be flawed. This should be re-evaluated as part of the HRA revision.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

310 The complexity of operator actions is assessed at two levels (simple or complex) based on the number of procedural steps, the level of workload and the degree of operator dependency. This latter factor is not explained, but from review of table 30-3 it appears to relate to between-person dependence, as a task is identified as 'complex' where more than 1 person is involved. The assessment of complexity is made in relation to the complexity of the second task, and is consistent with the way in which the issue of complexity is dealt with in DEPEND HRA (Ref. 84).

311 The quality of procedural guidance is also assessed at two levels (clearly defined or not clearly defined) based on the need to transfer between procedures and the clarity of the procedural steps. It is not clear whether this assessment relates to the second, or both of the tasks being considered. However, in practice, a review of table 30-3 reveals that in all cases, quality of procedural guidance is assessed as 'clearly defined'.

312 The decision tree outlined earlier is not consistent with any published material that I am aware of that provides guidance for the assignment of dependency levels between HFEs in PSA. Whilst some of the factors appear in other techniques used for assigning dependency levels, they do not appear in the combination used in the UK AP1000 HRA, and for this reason the validity of the decision tree is questionable. Furthermore, the treatment of time in the decision tree is at variance with treatments of time in all other reviewed techniques for assessment of dependency levels. As discussed earlier the

important factor in determining the degree of dependence in relation to time, is not the difference between time available and the time required to perform the second task, but the time period between which the two tasks are required to be performed.

313 I judge that the methodology used to assign dependency levels between HFEs is flawed and I expect the dependency assessments be reassessed, particularly focussing on the assessment of the time between tasks.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

Assessment of Dependence within Cutsets

314 I have reviewed a number of dominant CDF cutsets in which multiple human error events occur. The aim of the review is to assess whether a dependent relationship is identified between events in the cutset, and where this is the case, that the level of dependence assigned is appropriate. Dominant CDF cutsets were identified from UKP-GL-GW-022, Chapter 33 (Ref. 67): Fault Tree and Core Damage Quantification. Table 33-3 in this document provides a cutset listing for core damage quantification for internal initiating events at power. Any cutsets related to SGTR however were not considered for assessment due to an identified weakness in the model for this event by my PSA colleague. From this table only 4 cutsets with different multiple HFE combinations were identified for assessment, and these are discussed below. As only a small number of dominant cutsets within the At Power PSA was identified, a review of the shutdown PSA dominant cutsets was also undertaken via UKP-GL-GW-022 Chapter 54 (Ref. 67). This identified a further 2 cutsets with multiple HFE that were subject to assessment.

At Power PRA Cutset 18 ATWS Precursor with no Main Feedwater

315 Cutset 18 has an ATWS precursor with no Main Feedwater as an initiating event. The cutset has an overall probability of $3x10^{-9}$ and contributes 1.25% of the CDF. Two HFE are included within the cutset, these are ATW-MAN03 operator fails to trip the reactor using the PMS within one minute (HEP $5.2x10^{-2}$) and ATW-MAN04C operator fails to trip the reactor using the DAS within one minute. Using the decision trees in Table 30-4 of UKP-GL-GW-022 chapter 30, the level of dependence claimed for ATW-MAN04C is high, and the conditional probability is calculated as $5.0x10^{-1}$, which provides an overall HEP of $2.6x10^{-2}$ for the HFE in the cutset. Whilst the level of dependence assigned is correct based on application of the decision tree shown in Table 30-4, there is no clear evidence to support the argument that the operating team will be able to recognise the need for manual scram in the time available. This would require the following sequence of events to be completed: attempt the scram using the PMS; recognise that PMS has been unsuccessful; and attempt manual scram using the DAS within one minute. Given the extremely short timescale for the required human actions I would expect to see strong evidence that event ATW-MAN04 is not completely dependent on ATW-MAN03 - currently this is not provided by the dependency level evaluation. I have considered the feasibility of the claimed actions for ATW-MAN03 in my Work Stream 1 assessment. This concluded that the timescale of one minute is not substantiated by the qualitative evidence presented by Westinghouse.

At Power PRA Cutset 33 ATWS Precursor with Main Feedwater

316 Cutset 33 has an ATWS precursor with Main Feedwater as an initiating event. The cutset has an overall probability of $6.95x10^{-10}$ and contributes 0.29% of the CDF. Two HFE are included within the cutset; these are ATW-MAN05: operator fails to trip the reactor using the PMS within seven minutes (HEP $5.2x10^{-3}$) and ATW-MAN06C operator fails to trip the reactor using the DAS within seven minutes. Using the decision trees in Table 30-4 of UKP-GL-GW-022, Chapter 30 (Ref. 67) the level of dependence claimed for ATW-MAN06C is high and the conditional probability is calculated as $5.0x10^{-1}$, which provides an overall HEP of $2.6x10^{-3}$ for the HFE in the cutset. In this event, in comparison to that represented in cutset 18, operators have a greater overall timeframe in which to perform manual scram, and hence there is a basis for the assignment of high dependency, rather than complete dependency between the two manual actions required to perform the scram.

At Power PRA Cutset 64 Small LOCA

317 Cutset 64 has a small LOCA as the initiating event. The cutset has an overall probability of $3.21x10^{-10}$ and contributes 0.13% of the CDF. Two HFE are included within the cutset; these are ADN-MAN01, operator fails to actuate the ADS for RCS depressurisation, as recovery from failure of automatic actuation (HEP $3.02x10^{-3}$), and REC-MANDASC failure to actuate the ADS for reactor coolant system depressurisation using DAS rather than PMS controls. A claim of high dependence is made for REC-MANDAS as discussed in Section 30.6.58 of UKP-GW-GL Chapter 30, and a conditional HEP of $5.06x10^{-1}$ is applied which provides an overall HEP of $1.53x10^{-3}$ for the HFE in the cutset. No substantiation is provided for the assignment of high dependency to REC-MANDAS; a blanket application of high dependency occurs wherever REC-MANDAS is identified to share a dependency with a preceding PMS activated action or diagnosis. Where REC-MANDAS is identified as a contributor to a significant cutset, I would expect a qualitative assessment of the particular recovery action to be conducted, to determine that the assumption of high dependence rather than complete dependence is warranted.

At Power PRA Cutset 66 Medium Loss Of Coolant Accident

318 Cutset 66 has a medium LOCA as the initiating event. The cutset has an overall probability of $3.06x10^{-10}$ and contributes 0.13% of the CDF. Two HFE are included within the cutset; these are LPM-MAN02: operator fails recognise the need for reactor coolant system depressurisation (HEP $3.3x10^{-3}$), and REC-MANDASC failure to recognise the need for reactor coolant system depressurisation using DAS rather than PMS displays. A claim of high dependence is made for REC-MANDAS as discussed in Section 30.6.58 of UKP-GW-GL-022 Chapter 30, and a conditional HEP of $5.06x10^{-1}$ is applied which provides an overall HEP of $1.67x10^{-3}$ for the HFE in the cutset. As discussed above I would expect a qualitative assessment to be conducted of the particular recovery action, to determine that the assumption of high dependence is warranted rather than complete dependence.

Shutdown PRA Cutset 12 Over Draining of Reactor Cooling System During Drain Down to Mid Loop

319 Cutset 12 has the over draining of RCS during drain down to mid-loop as an initiating event. The cutset has an overall probability of $2.18x10^{-9}$ and contributes 1.77% of the CDF. Three HFEs are included within the cutset: these are:

- RHN-MAN04: failure to recognise the need for and failure to isolate the RNS, given rupture of the RNS piping during hot/cold shutdown conditions (HEP 5.3x10-2);

- IWN-MAN00C: failure to recognise the need for and failure to open the IRWST motor-operated valves during shutdown conditions, given that the RNS is unavailable (Conditional Human Error Probability (CHEP) 1.5x10-1); and
- RHN-MAN05C: failure to recognise the need for and failure to initiate alternate gravity injection via the RNS hot-leg connection, by using the RNS line from the IRWST to the RNS pumps suction header (CHEP 1.5x10-1).

320 Thus an overall HEP of $1.19x10^{-3}$ for the cutset is derived. Whilst IWN-MAN00C and RHN-MAN05C are recognised as being dependent events and a claim of moderate dependency is made for the events in both cases, I can find no evidence in Table 30-3; Dependency Level Evaluation Summary, for the basis on which these dependency levels have been assigned. It should be clear on what basis moderate dependency has been assigned to the dependent events within this cutest, to provide evidence that the conditional HEPs used in the calculation are appropriate.

> ***AF-AP1000-HF-08*** *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

Shutdown Probabilistic Risk Assessment Cutset 24 Loss of CCS/SWS with Reactor Coolant System Filled

321 Cutset 24 has loss of CCS/SWS with RCS filled loop as an initiating even. The cutset has an overall probability of $3.82x10^{-10}$ and contributes 0.31% of the CDF. Two HFE are included within the cutest; LPM-MAN05: failure to recognise the need for RCS depressurisation during a shutdown condition, with failure of the CMTs and the RNS (HEP $6.83x10^{-4}$); and REC-MANDASC: failure to recognise the need for RCS depressurisation using DAS rather than PMS displays. A claim of high dependence is made for REC-MANDAS as per Section 30.6.58 of UKP-GW-GL-022 Chapter 30, and a conditional HEP of $5.06x10^{-1}$ is applied; resulting in an overall HEP of $3.46x10^{-4}$ for the HFE in the cutset. Again, I would expect a qualitative assessment to be presented to provide evidence that the assumption of high dependence is in fact warranted.

4.3.4.4 Human Error Dependence Conclusions

322 The basis of the treatment of HED in the UK AP1000 HRA is THERP. This is consistent with good practice and represents a well recognised and widely applied approach to the treatment of dependency in UK NPP risk assessment. The calculation procedures used for the derivation of CHEPs are consistent with those provided by THERP and the calculations I have checked are found to be accurate. Median HEPs provided by THERP are converted to mean values, which is a standard practice in the context of PSA.

323 Whilst THERP provides the basis for the treatment of HED, the dependency assessment is based largely on a series of assumptions rather than a dedicated task analysis in order to provide a substantiation of the dependency levels assigned. Such an assumptions based assessment requires substantial development as the safety case progresses, in order to provide evidence that the assumptions used have lead to a sufficiently conservative estimate of the human error contribution to the CDF for the proposed design. My review of the assumptions which underpin the dependency assessment suggest that this may not be the case.

324 HED in the UK AP1000 HRA is assessed at two levels: between subtasks in an individual HFE, in a manner akin to the use of a HRA event tree as described in the THERP handbook (Ref. 13), and between HFEs where multiple HFEs are found within a particular fault sequence or cutset.

325 Considering HED assessment within individual HFEs, the AP1000 HRA uses a number of assumptions to assign dependency levels of high, moderate or low and then uses the THERP dependency equations to derive conditional HEPs for the failure probability for the second subtask within pairs of subtasks, where paths are ORed to achieve success. As discussed earlier a number of these assumptions are problematic and have the potential to lead to an optimistic overall HEP for the HFE.

326 An overarching assumption related to dependency is provided by HRA Assumption C. This approach to dependency assessment is not consistent with the methodology for the assessment of HED as outlined in THERP handbook, where assessment of the level of dependence is recommended to be made between successive tasks. The assumption that a low dependency relationship will exist between the first and second operators' steps in a sequence of subtasks has potential for the derivation of optimistic conditional HEPs for the second sub-task. Further, the THERP methodology stipulates that dependency relationships should be assessed between successive subtasks not between the first subtask and all successive subtasks. However my review of the HEP derivations for individual HFEs presented in Section 30.6 of UKP-GW-GL-022 Chapter 30 (Ref. 67), could not find any evidence of the application of this assumption in the manner described above.

327 Assumption F relating to unproceduralised recovery is also considered to be problematic. This assumption is predicated on the judgement that recovery of control room operator error by the SRO or STA is best represented by THERP item "one-of-a- kind checking with alert factors" (table 20-19 item 3) and that this is modified by application of the low dependence equation (in the case of the SRO, but not the STA) from the THERP dependency model. Application of this item in my opinion requires a case by case assessment of the cues provided to the SRO and STA and the procedural requirements for checking. If this level of qualitative assessment is not provided, a more conservative approach to the assessment of HEPs for between person recovery should be taken in order to avoid optimistic overall HEPs for individual HFEs. A related assumption, assumption J, concerning unproceduralised recovery also uses table 20-19 item 3 to account for recovery of one operator error by a second operator where grace times for taking action are greater than one hour. This again is considered to be optimistic rather than conservative in the absence of detailed task analysis to provide evidence to substantiate the claim. The optimism in HRA due to the treatment of un-proceduralised recovery is evidenced in the HEP generation procedures for all HFE and therefore has a significant effect of underestimating the human error contribution to CDF in the PSA.

328 A further problem with Assumption F relates to the dependency levels assigned between the *RO* and SRO and the SRO and STA for emergency events. In the UK AP1000 HRA low dependency is assigned between the *RO* and SRO, and Zero dependence between the STA and SRO. This contradicts the levels of dependence recommended within THERP where high dependence is assigned between the *RO* and SRO and low to moderate dependence between the STA and SRO for diagnosis and high to complete dependence for post diagnosis actions. This has a significant impact on the conservatism of the HEPs generated in the HRA and should be addressed in any iteration of the PSA and HRA.

AF-AP1000-HF-09 *- The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.*

329 A third problematic assumption relates to the dependency levels assigned between primary and secondary cues available to operators to detect the need to take action or diagnose the appropriate course of action. Assumption L identifies that moderate dependency is assumed to exist between primary and secondary cues, however, this again may provide for optimistic HEPs particularly if primary and secondary cues are presented via the same interface, in the same form, to the same operator at the same or closely together in time. Therefore, without detailed task analysis of each case where multiple cues are credited, I would expect a more stringent dependency level to be applied, and this level to be reduced where evidence is provided by detailed assessment of the factors that reduce coupling mechanisms between the cues. This assumption appears to lack the level of conservatism I would expect from an assumptions-based analysis.

330 HED between HFEs is assessed using a series of decision trees, shown in Table 30-4 of UKP-GW-GL-022 Chapter 30 (Ref. 67), which evaluate four factors in order to assign a level of dependence between two related HFEs in a fault sequence or cutset. The origin of the decision tree used in the dependency level evaluation is not explained in the submission and is not consistent those provided in published methods for HED evaluation e.g. SPAR-H (Ref. 83) or DEPEND HRA (Ref. 84), although some of the factors found within the UK AP1000 decision tree are common with published schemes. On this basis further explanation is required of the logic underpinning the tree, particularly the choice of variables within it, in order that its validity can be assessed. The treatment of at least one of the factors used; time, is at variance with the way in which this factor is used in other methods for assigning dependency levels. This appears to be a fundamental error in dependency modelling which invalidates the between HFE dependency assessment.

AF-AP1000-HF-08 *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches for reasonably practicable design improvements to mitigate dependence mechanisms.*

331 Overall I consider that the approach taken to HED within the UK AP1000 HRA is inadequate. In the absence of detailed task analysis and substantiation underpinning the HRA, I find that the assumptions used to assign dependency levels within individual HFEs to lack sufficient conservatism. Almost all of HEPs are affected by this overarching conclusion; resulting in a HRA that is likely to be optimistic. With respect to the assessment of dependence between HFEs, I find the approach to the treatment of the dependency coupling mechanism of time in the decision tree shown in table 30-4 of UKP-GW-GL-022 chapter 30 (Ref. 67) to be fundamentally flawed. On this basis it must be concluded that the treatment of between HFE dependence is unreliable and requires significant revision in a subsequent iteration of the HRA and PSA.

AF-AP1000-HF-08 *- The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment that searches*

for reasonably practicable design improvements to mitigate dependence mechanisms.

4.3.5 Conclusions

332 It is clear that there are many and considerable issues with the current AP1000 HRA. Both myself and my PSA colleague highlighted problems with the model at the end of GDA Step 3, and the work that I have undertaken during Step 4 has amplified my judgement that the HRA should be fully revised. I recognise that the qualitative HF assessment work undertaken by Westinghouse to develop the HF safety case for the AP1000 has not been reflected in the HRA; and as the safety case and supporting risk assessments move forward those analyses should be fully incorporated to the revised HRA model. I question the general applicability of THERP and early consideration should be given to the appropriateness of THERP to the revised HRA. I do not consider that the current model represents recognised good practice in terms of quantitative HRA, and that this is largely a result of the age of the model; its incompleteness and all of the modelling issues that I have highlighted here.

333 My judgement on the quality of the HRA aligns with that of my PSA colleague at the end of Step 4; that there are substantial weaknesses in the HRA model, resulting in the requirement for a complete revision as the risk assessment for the AP1000 progresses beyond the PCSR stage. This requirement is cited as an Assessment Finding; as my judgement is that the integrity of the HRA risk model will not have a significant impact on the design of the AP1000, or the overall acceptability of the PSA. One could suggest that the inherent weaknesses in the model represent a significant gap in the safety submission and hence may require resolution prior to issue of a DAC; however it is my judgement that the qualitative weaknesses in the safety case for HF (refer to Section 4.2 of this report) represent the most considerable safety gap and are most likely to impact the design of the AP1000. Furthermore, quality and completeness of the qualitative analysis is required to underpin the HRA revision.

4.4 Work Stream 3: Engineering Systems - Assessment

334 In the HF safety case (Ref. 35) Westinghouse makes the claim that: *"Operator actions that degrade or prevent systems from performing their safety functions have been identified (i.e. maintenance latent errors). These operator actions have been assessed to ensure that the contribution to risk associated with their occurrence will be ALARP"* (Claim 1.2.2 Ref. 35). This claim is supported by a series of arguments; the principal one of which is:

"The design, operation and maintenance tasks of the safety systems and risk mitigation systems have been reviewed and steps have been taken to improve the design to prevent and minimise maintenance induced initiating events and latent maintenance errors." [Argument 7, Ref. 35].

335 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 specifically considered the Squib valves (as a 'novel' technology for UK NPP safety systems), and briefly considered human reliability issues associated with software maintenance and metrication.

4.4.1 Maintenance / Maintainability

336 These findings relate to item (1) from the methodology and scope presented in Section 2.2.7.2. Westinghouse categorised and prioritised their HF effort according to three areas: 'Core': areas in which rigorous HF input and methodologies are required (approximately 70% of HF effort); 'Adjunct': areas in which the *HFE* function has a comparatively substantial role in the design process, but not the primary responsibility (approximately 25% of HF effort); and 'Peripheral' - areas where there is limited operator involvement and the tasks are not related to safety. HF input is primarily through design guidelines (approximately 5% of HF effort).

337 In addition to this, Westinghouse determine the precise nature and level of HF involvement based on the:

- degree of human involvement in the task;
- nature of the task (task complexity, required speed of operator response);
- potential safety or operational consequences of an operator error;
- knowledge of the AP1000 design; and
- input from others in the AP1000 project.

338 Westinghouse provided indicative areas associated with each category (for example the MCR design is considered a 'core' area, and operations support areas and plant areas that indirectly sustain MCR operations are considered 'adjunct' areas). Westinghouse did not provide a definitive list of systems categorised as either 'core', 'adjunct' or 'peripheral' as all components within a single system do not necessarily fall into a single category; therefore I cannot be confident in the level of formal *HFE* applied to particular systems of interest. However from a review of the HF Engineering Programme Plan (HFEPP) (Ref. 85), it appears that 'maintenance' activities and areas are generally considered to be a peripheral area; and hence are not afforded a dedicated and formalised HF input (for example: *"Examples of peripheral areas include control workstations and panels located in the field that are used for simple, infrequent, and/or maintenance tasks."* And: *"The human factors aspects of the plant layout, room layouts and equipment design for operations and maintenance are designated as peripheral human factors areas."*). I also note however that there are particular areas and systems that were considered in more detail from a HF perspective; for example the Squib valves. Westinghouse also cite the maintainability HF engineering assessment (Ref. 86) as an 'adjunct' level of HF input relating to maintenance.

339 There is therefore some evidence of a systematic and appropriate HF integration into maintenance activities and areas, although I judge that overall this is in the minority. Ordinarily from a risk perspective, this may not matter a great deal, however in a system such as the AP1000 with sophisticated engineered systems; I expect recognition of the potential transfer of human error from post fault actions to maintenance type activities.

340 In terms of the type of HF analyses applied to maintenance activities and areas, Westinghouse cite the task analyses associated with safety important maintenance tasks. The OSA summary report (Ref. 87) highlights the findings from the analysis of 38 Maintenance, Test, Inspection and Surveillance (MTIS) tasks judged to have some risk importance.

341 I recognise that the HF safety case for the AP1000 (Ref. 35) provides HF analysis of 69 maintenance tasks (refer to my Work Stream 1 assessment earlier), and the analysis submitted in December 2010 in response to my RO-AP1000-090 (Ref. 76), provides more

detailed error identification analysis of two of the 69 tasks. As stated earlier, I have not had sufficient time within GDA Step 4 to consider the RO-AP1000-090 work in any detail, and that this forms part of the corresponding GDA Issue Action. However, from a very early appraisal of this work, it appears that there is an insufficient focus on design issues, and the contribution of the system design to reducing the potential for human error in maintenance tasks to ALARP.

342 Westinghouse also cite the Maintainability HF Assessment (Ref. 86) as further evidence of the HF contribution to maintenance human reliability. This document lists around 70 safety significant components for assessment using 3D models, evaluation based on design documents and drawings, discussion with NPP engineers and operators, assessment on physical equipment and/or participation in discrete maintainability studies. I note that the scope of this work seems reasonable, but that the focus was a review of system design against the 'maintainability guidelines' (Ref. 88), and I do not have information on how the judgements of compliance with the guidelines were made. There was not an explicit human error focus in this work.

343 In terms of the contribution of (HF influenced) design to the ALARP position for maintenance tasks, Westinghouse state (Ref. 88): *"Components will be designed to be robust and resistant to anticipated impacts and accidents. Protective devices are fitted to protect vulnerable components, but care should be taken in fitting and removing them so that they do not cause damage to the component. The maintenance crews should report any accidental damage and will be aware of the penalties of failing to do so. Components are designed to be easy to remove and refit. Where possible, components are designed to be easily accessible and can only be fitted in the correct orientation. Nuts and other fasteners will be easily accessible. Design for access, movement of equipment and other maintenance issues are the subject of a maintainability study. Some of the issues raised in that work such as the application of manual force and labelling are the subject of later study to be done"*. This appears to be a largely prospective position, rather than an evidence based contribution of the integration of HF to the design of maintenance tasks and equipment, to reduce the human error potential to ALARP.

344 The proforma analysis submitted as part of the HF safety case (Ref. 35) do consider how the risk from latent human failures can be further reduced, however this is within the task; i.e. the analysis presumes that the task will be manual, and seeks to optimise the task within that framework. What appears to be missing is evidence of the optioneering of MTIS tasks, including the potential for automating MTIS tasks. This relates to an earlier finding relating to the apparent lack of an overarching ALARP justification.

> ***AF-AP1000-HF-28*** *- The licensee shall reconsider the requirements for manual maintenance, and demonstrate that appropriate consideration has been given to alternative options including the feasibility of automation; in line with SAP EKP.5 and our ALARP requirements.*

345 To optimise equipment design from a maintenance perspective, Westinghouse has also developed the 'Local Panels and Maintainability HF Design Guidelines' (Ref. 88), which aims to provide HF guidance to engineers. I reviewed the guidelines and found them to be broadly compliance with recognised good practice. The exceptions that I noted are that the hand access requirements do not recognise the potential wearing of PPE and the guidance relating to fault identification and diagnosis appears to be limited. I also note that the source documentation is largely US focused, and there is no explicit mention of recognised British Standards, such as that on the 'maintainability of equipment' (Ref. 89),

however this is a minor point and in general I judge that the guidance is sufficiently comprehensive.

346 I note minor observations relating to the applicability of the guidance; there is no instruction on how to determine which aspects of the guidance might apply to the equipment design in questions; how trade-off between guidelines would be managed, and the guidance is not graded in terms of mandatory and discretionary guidance for example. However I judge that a professional design engineer applying his judgement would consult HF engineers as required.

347 My main assessment point relating to all of the design guidance applied by Westinghouse is that it is US focused and recognises US national population stereotypes. There are recognised conflicts between US and UK population stereotypes (on/off - up/down being one of the most obvious), and in light of this Westinghouse commissioned research in this area. This is discussed later under my Work Stream 5 programme of work, and has an associated Assessment Finding.

> ***AF-AP1000-HF-29 -*** *The licensee shall review the Westinghouse work on UK national population stereotypes; provide an impact assessment on the generic design of HMIs and justify how the UK AP1000 final interface designs comply with national population stereotypes. This should also form part of the V&V programme.*

348 There is additional evidence of the HF contribution to maintainability via the Design Change Process (DCP), and I accept that HF has made a contribution to changes in the plant and equipment design through applying this process. There is also the Constructability, Operability, Maintainability, Inspectability and Testability (COMIT) workshop process, which involves a multidisciplinary review of the 3-D CAD plant model to determine the ease of maintainability and replacement of system components, from the perspective of space and access. HF is one of the COMIT discipline participants.

349 I note the substantial Operating Experience Reviews (OERs) undertaken by Westinghouse, and the potential for that work to provide insight into maintenance activities. However my review of this highlighted that there was not an explicit focus on maintenance work. I consider this to be a missed opportunity rather than a point of assessment note.

350 It is my judgement that Westinghouse has integrated HF into maintenance activities and recognise the importance of maintainability, but that the focus has been limited. There is a lack of systematic human error analysis for a sufficient range of safety important systems, and this will be taken forward as part of GDA Issue Action HF1.A1. I further consider that there is a lack of evidence relating to an overarching process to determine those tasks for which manual maintenance is the ALARP position. Again this is to be taken forward as part of GDA Issue Action HF1.A1. I acknowledge that the proposed validation and verification activities will provide an opportunity to further investigate maintenance design issues, as part of the overall Design Verification Plan (Ref. 90). It is my expectation that as the safety case progresses beyond the PCSR and into the Pre-commissioning Safety Report (PCmSR) phase, a potential licensee should ensure that their validation and verification activities adequately consider maintenance/maintainability.

> ***AF-AP1000-HF-30*** *- The licensee shall specifically include maintenance and maintainability issues in their Human Factors V&V programme.*

4.4.2 Consideration of Novel Engineered Systems

351 These findings relate to item (2) from the methodology and scope presented in Section 2.2.7.2.

Squib Valves

352 A squib is an explosive mechanism, used in a range of devices such as aircraft ejector mechanisms; missile firing mechanisms; missile fuel supply systems; car airbags and fire extinguishing systems. This type of device, although well understood in other industries, is considered a novel technology in the UK NPP industry, particularly because of the size proposed by Westinghouse.

353 The squib forms part of the ADS staged safety system (stage 4). They are activated automatically when the water level in the CMTs falls below 20%. Earlier ADS safety stages (1-3) (e.g. when the CMT level is at the 67.5% fluid level) employ motor-operated valves.

354 The valves employ one-off explosive devices, and hence testing of the valves to assure reliable detonation is challenging. There is an extant Failure Modes and Effects Analysis (FMEA) available (Ref. 174) that identifies squib valve failure mechanisms. However, although I have not reviewed this, mechanical engineering colleagues have, and have included a requirement for it to be reviewed and updated as part of one of their GDA Issue Actions (GI-AP1000-ME1 refers).

355 The novelty of the large squib valve application to UK NPP safety systems, led to the decision to carry out a more detailed assessment of the extent and adequacy of HF support to the squib valve design and maintenance.

356 Westinghouse state that the decision to use squib valves was originally made because they rely less on operator intervention (to open valves etc); are virtually leak free and are considered to be more reliable than other types of valves.

357 Westinghouse provide data that claims that squib valves are more reliable than air or motor operated valves, estimating a failure probability of: 5.8×10^{-4}. This is a purely mechanical failure probability on demand, and I understand that my mechanical engineering colleagues are not questioning the derivation of this value. The Westinghouse assessment of the human unreliability associated with the squib valve maintenance derives a HEP of 6.0×10^{-5} (refer to Westinghouse proforma OPR-011 in Ref. 35). However I consider this value optimistic, and using my own qualitative assessment of this task (Ref. 77), I calculate that a HEP of 1.2×10^{-2} is more appropriate (refer to the calculation in note in Annex 6). When combined with the mechanical failure probability, this results in an estimated overall probability of failure for the squib of 1.25×10^{-2}.

358 Westinghouse state that that the squib valve has design features to reduce the likelihood of maintenance errors and resulting operating deficiencies. A key design feature is the way that components (to be removed for inspection and replacement) have been constructed; following the principles of Poka Yoke design (failsafe or mistake proof design). Essentially they are built in such a way to ensure that re-installation cannot be carried out incorrectly. In the Squib Valve Design Project Summary (Ref. 91), Westinghouse cite the following examples of Poka Yoke design employed on the squib valve to help reduce maintenance errors:

- Each tension bolt type has a different thread size, which ensures it is fitted to the correct piston and valve bonnet.

- Each piston type therefore has a specific size tapped hole, which ensures the correct tension bolt is fitted.
- Each valve bonnet type therefore has a specific size tapped hole, which ensures the correct tension bolt is fitted. In addition the cartridge well is different for all three cartridge types, which ensures the correct type of cartridge is fitted.
- Each cartridge type has specific external parameters, (diameter and height) that ensure the correct fitting of a cartridge to a specific valve bonnet.
- Each shear cap is positioned within the valve body by bolts, which are on a specific PCD to suit the valve type. In addition the valve body has specific tapped holes to suit specific shear caps.
- The 8 inch valve body contains an arrow to indicate flow direction on its external surface to ensure each valve is fitted into plant in the correct orientation.

359 I therefore judge that Westinghouse has employed elements of recognised good practice to the design of the squib valves, to aim to reduce the human error potential to ALARP; although this is not necessarily evidenced through a formal HF integration process.

360 I have not considered the operator response to a spurious squib valve actuation or the likelihood of that occurring. Westinghouse has not provided a safety case for such an occurrence. My colleagues in Fault Studies and C&I have explicitly considered this and through GDA Issue GI-AP1000-CI-04 they require that Westinghouse provide a deterministic and probabilistic safety case for such an occurrence. Any resultant claims on operator action will require justification.

361 I acknowledge the lack of violation potential relating to squib valve actuation as there appears to be no manual means for an operator to prevent their automatic actuation.

Software Maintenance

362 The AP1000 incorporates more automated systems and Visual Display Unit (VDU)-based soft controls, than earlier generation UK plants. This typically presents different (latent) human error modes for consideration and mitigation. My interest lies in 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 Westinghouse is applying an established software development system that recognises the potential for human error and provides mitigation opportunity. Westinghouse stated in response to TQ-AP1000-563 that *"The CSDP [Computer Software Development Process] is structured to meet the intent of IEEE/EIA 12207.0-1996* (Ref. 175) *regarding software lifecycle processes. This standard recognises HF in the software development process in both the System Requirements Analysis and Software Requirements Analysis activities"*. This is consistent with the judgement of my C&I colleagues.

363 Post GDA my interest will relate more to the control of software upgrades and changes. I have worked with my C&I colleagues to understand the software development process and standards employed by Westinghouse. With their help I have gained a level of confidence that the standards employed by Westinghouse typically provide opportunities for human errors to be identified and recovered. I am also assured that the prescribed off-line channel based testing and the statistical testing (post PCSR expectation) provides additional human error identification and recovery opportunity. Therefore at this stage of the risk assessment I do not consider that there are any HF issues associated with the Westinghouse approach to the development of the first installed software process.

Metrication

364 I recognised the potential human (un)reliability issues associated with the proposed Westinghouse 'quasi-metrication' strategy, and provided input into this cross-cutting GDA concern. The human reliability issues are clear, and from my perspective it is not acceptable to design and operate a plant with mixed units. To illustrate the issues I have undertaken a brief review of the accident literature to identify experience where errors associated with mixed units have resulted in unacceptable consequences. This is reported in Ref. 77. I support the proposed GDA Issue in this area (GDA Issue GI-AP1000-ME-02 refers, see Ref. 178).

4.4.3 Conclusions

365 In general I judge that Westinghouse has attempted to address the human reliability aspects of maintenance; and there is evidence of analysis and design input to support their claims in this area. However there are significant gaps in the HF contribution that I am taking forward as part of GDA Issue Action HF1.A1.

4.5 Work Stream 4: Human Factors Integration - Assessment

366 This assessment has drawn upon over one hundred reference documents, and uses TAG T/AST/058 (Ref. 7) and SAP EHF.1 (Ref. 4) as its basis. The HF safety case claims that the *"Human Factors Programme Plan has been used to define a human factors engineering program for the AP1000 plant. The program is being executed in order to integrate the comprehensive scope of human factors good practice to the design of the AP1000"*.

367 In general I judge that Westinghouse has evidence of a *HFE* programme of work; but it is just that; a HF engineering scope of work, which is in itself limited by their programme and resource split into core, adjunct and peripheral elements. This split is risk based and does not take explicit account of complexity and novelty; and does not necessarily result in an ALARP position. 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.

368 A recognisable HFI plan will be required for any UK AP1000 construction; which amplifies the current *HFE* programme, which was essentially produced in response to US regulatory expectations.

> ***AF-AP1000-HF-31*** *- The licensee shall develop and submit a HFIP for UK AP1000 construction.*

369 In the HF safety case (Ref. 35) Westinghouse make six claims and sub-claims. These are supported by associated arguments and suggested evidence. The nature of HFI is such that it relates to the entirety of the plant design and analysis. Therefore the overriding claim that: *"The role of the operators in ensuring nuclear safety in the AP1000 has been minimised"* (Claim 1.0 Ref. 35) has the greatest relevance to Work Stream 4.

370 This section explores the robustness of these claims and arguments against the evidence presented.

4.5.1 Scope of Human Factors Integration (HFI)

4.5.1.1 Breadth of Human Factors Integration Programme

371 Westinghouse presents their HFEPP (Ref. 85) as their HFI proposal. I have considered this together with the DCD (Ref. 64) and the UK HF safety case (Ref. 35) to assess the scope of their HFI proposals. In this section I essentially consider the presence of the expected work item, rather than comment on the quality of what has been achieved. The review is against the components cited in our HFI TAG T/AST/058 (Ref. 7); refer to Table 15 below.

Table 15: T/AST/058 Elements against Westinghouse Position

T/AST/058 Element	Westinghouse Position
The strategy for integrating HF	This is described within the boundaries of C&I, but only to a limited extent outside that
A project organogram	An organogram is provided
The work breakdown structure	This is provided, and there is a sizeable programme of *HFE* work within the approach to allocation of resources (core, adjunct, peripheral)
Integration of HF within the project plan	Key HF deliverables are provided, but no dependencies
HF SQEP resource requirements	These and their management are provided
The HF standards to be applied	These are provided
How assumptions, uncertainties and project issues and risks will be managed and resolved:	I have not found any discussion of assumptions and uncertainties. Issue management is presented
How trade-offs between different discipline requirements will be managed and resolved:	I have not been able to determine the day-to-day working arrangements for trade-offs
Hold points and design reviews and the expected HF	This is provided
Ownership of particular aspects of the work	Responsibilities are defined
Progress monitoring arrangements	These are not provided
Reporting methods	This is provided

372 In summary, the Westinghouse programme meets the major elements of the HFI TAG (Ref. 7), although I note that the programme only relates to their 'core' elements. I further note that there is UK HF safety case (Ref. 35) material not cited in the HFEPP (Ref. 85), and that it has not been updated to reflect more recent work such as the layout reviews.

373 I also reviewed the HFEPP (Ref. 85) against the technical expectations cited for PCSR in TAG T/AST/058 (Ref. 7). I note that all of the work packages are essentially included, with the exception of link analysis and assumptions and trade-off resolution. I also note the omission of project level metrics that track compliance with HF requirements and guidance. Although this is not an explicit expectation cited in our TAG; it is a recognised

good practice within HFI, and transparently demonstrates compliance and trade off resolution.

4.5.1.2 Technical Scope of Work

374 I assessed the HF and its 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 Westinghouse has in place to deliver quality HF work; and this is reported in Table 16. Items not within the scope of my other assessment work streams are explicitly considered in more detail outside of Table 16.

Table 16: Assessment of Westinghouse Processes for Delivering HF Work

Technical Area	Commentary on Adequacy of Westinghouse Processes for Quality Delivery
Job design	Westinghouse consider this an issue for a prospective licensee; and makes assumptions in the UK safety case regarding job roles, principally for the MCR staff (for further comment Section 4.6.8 refers). These roles do not appear in the Concept of Operation but do appear in the "AP1000 Main Control Room Staff Roles and Responsibilities" document (Ref. 176). Task analysis and engineering tests have been performed to assess the roles; which is what I would expect. Westinghouse has not presented analysis of plant staffing levels; and I consider this an omission to be addressed as the safety case develops. ***AF-AP1000-HF-32 - The licensee shall provide a justification of the minimum staffing levels proposed.***
Competency and Training	Westinghouse applies a job and task analytical (JTA) approach to competency and training; yet there is no rationale for the choice of JTA. Using IAEA guidance (Ref. 104) it would appear that job competency analysis may be more appropriate for the tasks involved. However from a process perspective I have no significant issues with the approach adopted.
Task Analysis	Westinghouse applied a staged approach to their task analysis and employed recognised methods. From a process and scope perspective I have no issues with the Westinghouse approach; the high level aims of the Westinghouse programme cover the main areas that I would expect to see from such a programme. A prospective licensee should consider additional task analytical requirements relating to non 'core' areas on a proportionate basis. ***AF-AP1000-HF-33- The licensee shall undertake, or justify otherwise, additional task analysis relating to non 'core' areas on a proportionate basis.***
Allocation of Function	Initial functional allocations were based on Westinghouse PWR reference plant; and those functional allocations were applied to the AP600 concept design. Westinghouse then argues that the same baseline functional allocation applies to the AP1000. Hence the AP1000 AoF case is based on Westinghouse PWR reference design. From a process perspective

Table 16: Assessment of Westinghouse Processes for Delivering HF Work

Technical Area	Commentary on Adequacy of Westinghouse Processes for Quality Delivery
	this appears flawed in that there have been significant technology advances since the era of the reference plant design; which may result in different baseline AoF to be considered. However Westinghouse has provided detailed assessments of the functional allocations and these are considered under my Work Stream 5. Again, from a process perspective, I am broadly satisfied with the method applied to these detailed assessments.
Workplace Design	The workplace design activity has been largely restricted to the control room areas. The Main Control Area (MCA) layout was developed during a HF-led workshop with utility input. A wide range of design options were considered; assumptions were documented, and utility concerns with the original design documented. A set of criteria were developed, and the voting procedures appear professional. The approach taken to the Operational and Control Centres System (OCS) workplace design represents good practice and I have no significant concerns. I have largely been unable to asses the design process outside of the OCS as there appears to be limited evidence available; I do however note informal signs of good practice that appear to have resulted without a formal HF contribution.
Physical and Environmental Ergonomics	From a process perspective I have no significant issues with the approach taken to the design of the physical and environmental work spaces. However I do have a concern with the appropriateness of the anthropometric data applied; as discussed in my Work Stream 5 assessment. ***AF-AP1000-HF-34 - The licensee shall justify the anthropometric data source applied to physical design of the AP1000 on a proportionate basis, against recognised UK data sets. This should recognise reasonable estimates of the secular trend of the intended operating lifetime of the plant.***
Control / Display Design	I considered the process for ensuring HFI to the design of plant user interfaces. This is largely achieved via the HF guidelines (Ref. 105); which I have reviewed and consider to be lacking in terms of their mandatory scope. They also lack a clear interface with other related disciplines. I also consider that the guidelines lack a formal status in terms of auditing and requirements on suppliers; Westinghouse state that they are '*considered*' part of the Quality Management System (QMS). The Westinghouse labelling procedure appears logical, and the OCS functional requirements document offers some confidence that the OCS will meet user requirements. I am less assured about the HFI to the design and procurement process for local control panels, bought-in equipment and Commercial Off The Shelf (COTS) software, in that there is a lack of evidence of any HF input. From a HFI perspective, I expect a prospective licensee to include the usability of local to plant interfaces as part of their V&V programme.

Table 16: Assessment of Westinghouse Processes for Delivering HF Work

Technical Area	Commentary on Adequacy of Westinghouse Processes for Quality Delivery
	AF-AP1000-HF-35 - The licensee shall include the measurement of the usability of local to plant interfaces as part of their V&V programme.
Procedure Design	From a process perspective, it is clear that Westinghouse has a significant procedure development and authoring system in their QMS. My only concern of note is the standards that have been applied to the design of the Computerised Procedure System (CPS). NUREG/CR-6634 (Ref. 177) is now dated, and computer display technology has developed significantly in the past decade. A prospective licensee should consider the standards applied to the design of the baseline CPS system, and provide a benchmark against current, recognised good practice in this area. ***AF-AP1000-HF-36 - The licensee shall provide a benchmark against current recognised good practice for the design of the baseline CPS system.*** I also note that there is no HF contribution or provision for contribution to the design of technical manuals; and this should be reconsidered on a proportional basis by a prospective licensee. ***AF-AP1000-HF-37 - The licensee shall include HF requirements and good practice in the design of technical manuals.***
Administrative Controls	There is no provision for HF consideration of an administrative control system within the Westinghouse HFEPP (Ref. 85). I accept that this is largely an issue for a prospective licensee organisation; however I would expect a process provision to be highlighted in the HFIP, and for the Administrative Controls that are designed to keep operations within the Safe Operating Envelope to be identified at the (site specific) PCSR stage ***AF-AP1000-HF-38 - The licensee shall include in their HFIP the requirement to develop an administrative control system.*** ***AF-AP1000-HF-39 - The licensee shall identify and justify administrative controls that are required to maintain operations within the Safe Operating Envelope, at site specific PCSR stage.***
Design for maintainability	From a process perspective I note the recent HF contribution to work on maintainability. In general I consider the scope of the formal HFI to be limited; however I do accept the more informal approach of seeking user input via ex-maintainers.
Design for decommissioning	Westinghouse state in their HFEPP (Ref. 85) that: "*The decommissioning stage is not included as it is far removed in time from the implementation of the HFE Program Plan"*. However the Westinghouse Decommissioning Summary Report (Ref. 106) does contain proposals that include consideration of HF aspects. However I have been unable to determine whether these have been implemented, or whether compliance with them in the design has been assessed. Therefore I suggest that prospective licensee reviews the HF contribution to the design for decommissioning.

Table 16: Assessment of Westinghouse Processes for Delivering HF Work

Technical Area	Commentary on Adequacy of Westinghouse Processes for Quality Delivery
	AF-AP1000-HF-40 - The licensee shall review the HF contribution to the design for decommissioning.

Concept of operations

375 The HFI TAG describes the typical content of a concept of operations document. I reviewed the Westinghouse document against this and determined that there are significant omissions and shortfalls. The main issue relates to the staffing concept; which is poorly defined, and although I accept that this is largely an issue for the prospective licensee, Westinghouse should be clear what can and cannot be achieved with the range of staffing options as part of the risk assessment and safety case, i.e. there should be a demonstration that the design can support the range of staffing options being considered. Table 17 below considers the broad expectations cited in the TAG with the Westinghouse position:

Table 17: T/AST/058 Expectations Related to Concept of Operations Definition against Westinghouse Position

Typical Content of a Concept of Operations (TAG 058 refers)	Westinghouse Position
Statement of the operational purpose of the system	Not explicitly defined. My concern here relates to the treatment of conflicting goals and the management of conflicting priorities
Consideration of the command and control philosophy	Some shortfalls; the treatment of incident management is at an early stage.
Staffing concept and their capabilities and responsibilities	There does not appear to be a discrete Target Audience Description (TAD); but there is a list of job roles in the job and task analysis and the AP1000 Concept of Operation (Ref. 140) provides details of proposed staffing under different conditions.
Basic details of the working environment	Provided for the 'core' programme.
Work organisation and design	As defined by the staffing concept and with limited consideration outside of the MCR roles.

Validation and Verification

376 The majority of US and China V&V is still to be performed. Westinghouse describe their generic approach in the 2003 document: 'Programmatic Level Description of the AP1000 Human Factors Engineering Verification and Validation Plan' (Ref. 108): *"The V&V scope will be limited to those facilities required for scenario evaluation that involve risk-important tasks, as defined by the PRA threshold criteria. Facilities included in the V&V scope are:*

Main control room Remote shutdown workstation technical support center (TSC). ...The AP1000 design does not require risk-important actions to be taken from local control stations, so local control stations are not included in the V&V scope. If, as a result of further analysis, risk-important tasks or critical actions are identified at local control stations, those stations, with respect to the identified tasks or actions, will be included in the V&V." The Integrated Systems Validation (ISV) (Ref. 109) is also restricted to the MCR.

377 I do not consider that this restricted scope is an ALARP approach. Westinghouse has subsequently provided much greater definition and detail of their approach to V&V in a suite of plans, e.g. Ref. 90. UK prospective licensee organisations should take account of the scope, content and findings of this planned activity to inform their own V&V as part of their PCmSR.

> ***AF-AP1000-HF-41 -*** *The licensee shall justify or redevelop the scope of the Westinghouse proposals for V&V and ISV.*

378 There have been earlier V&V type activities, including various engineering and man-in-the-loop tests to inform the design. There were also simulator trials in the mid 1990's that I have not examined. The approach described in the man in the loop document (Ref. 110) I consider is well-founded, with an understanding of the technology, MCR design issues, and evaluation. Engineering tests have been planned, conducted and reported to a high professional standard, including an adequate range of measures (activity, workload, errors and comments) and good trials control.

379 I have some concern over the conduct of the engineering tests in terms of the examination of team-working. The Phase 2 trials focused on the comparison of 2-man vs. 3-man staffing. The Phase 3 trials used 3-man staffing, but did not introduce an STA. The aspect of teamwork that would link to the safety case is the potential for error recovery within the crew; indeed there is no explicit link between the engineering tests and the PSA (e.g. examining HRA assumptions). I also note that the tests have not been used as an opportunity to validate the task completion times in OSA-2 (Ref. 87). I expect these omissions to be addressed as part of the UK V&V and ISV programme.

> ***AF-AP1000-HF-42 -*** *The licensee shall specifically include in the UK V&V and ISV, testing of the MCR staffing proposals and validation of the task completion times offered by Westinghouse in OSA-2.*

Design Reviews

380 There are various design checklists relating to HF for application during design reviews. I reviewed six system design review documents for 5 systems to determine the HF contribution; Table 18 refers:

Table 18: Human Factors Contribution to System Design Review

System	Design Review	Checklist	Comments
PMS	Intermediate	HF, Repairability and maintainability	HF attendance. Three questions related to HF in the review criteria.

Table 18: Human Factors Contribution to System Design Review

System	Design Review	Checklist	Comments
CVS	Preliminary	Safety and Human Performance Q1	Repairability and maintainability checklist not used, despite considerable discussion of the topics
Primary Sampling	Intermediate	Safety and Human Performance	Utility attended. 'Intend to comply' to local panel guidelines. Utility Requirements Document (URD) requirements include operability requirements. AP600 maintainability issues now closed. Open Item raised to add references to Operator Actions including task analysis
Feedwater	Preliminary and Intermediate	Repairability and maintainability Safety and Human Performance N/A	None
Accumulator tank	Final	Repairability and maintainability Safety and Human Performance	Utility attendance. FMEA includes human error.

381 I also examined a design review with a sub-contractor; the Polar Crane Intermediate Design Review. This review had been highlighted by Westinghouse (response to TQ-AP10000-1110) as having received HF consideration. The design review compliance matrix included a number of items related to HF, but there was no reference to formal HF documents such as the HF guidelines, or to HF activity. Topics related to HF were raised in the review and actions were completed. From the point of view of engineers considering the user, this is a good common sense approach.

Utility and User input

382 There is evidence of considerable formal and informal use of utility input, including design reviews, engineering tests, bench tests, CAD model reviews and the Builders Group; representing good practice. There are also many ex-operators employed by Westinghouse to support the operational aspects of design (in an informal manner it appears). They are deployed in the HF and operations group, the procedures writers group, the training group, and the simulator development group (and others). Display design has also had an operations lead. 'Operations Experts' with defined qualifications have specified roles and responsibilities in the Display and Operations Work Group.

4.5.2 Integration and Implementation

383 This section considers the evidence for HFI across sampled aspects of the AP1000 project.

Integration with the Safety Case

384 There is evidence that there has been a flow of information between the HRA and *HFE*; it is clear that the HRA results have driven the selection for scenarios for detailed task

analysis and have inputted to the design of the Human System Interfaces (HSIs), procedures and training programmes. However, what has not occurred is the reverse; the re-examination of HRA assumptions as a result of HF work, which Westinghouse state will occur when the PSA is revised. I also was not able to determine evidence of a link between PSA system unavailability goals and estimates of maintenance times; which I expect a prospective licensee organisation to address.

> ***AF-AP1000-HF-43*** *- The licensee shall provide estimates of maintenance times linked to the PSA system unavailability goals.*

Application of Task Analysis

385 There is evidence of the requirement for and use of task analysis to inform Human Machine Interface (HMI) design via numerous display design documents. There are high level requirements for the use of task analysis into systems design. Westinghouse has placed high level requirements for the implementation of the Function Based Task Analysis (FBTA) as functional displays, and for the main sub systems to be based on the task analysis, but it is not clear how the latter is to be achieved.

386 I examined the functional requirements documents to identify their task analysis input. There is no task analytical input to the alarm system, CPS or WPIS functional specifications. There are line references to task analysis in the PMS specification, but no task analysis documents referred to or cited.

387 I was not able to determine any evidence relating to task analysis requirements for adjunct or peripheral systems or equipment.

Integration to Design

388 I sampled ten SSDs to examine implementation of the HSI guidelines (Ref. 105) and the Local Control Panel Guidelines (Ref. 88). Table 19 below indicates the extent to which the guidelines were applied. In some instances a guidelines document would appear in the list of references but would not be cited in the text. In other instances, the document was called up as a requirement, while in others it was not mentioned at all. Two systems did not mention either document. One system called up both documents. Five systems called up the Local Control Panel Guidelines (Ref. 88).

Table 19: Implementation of Human System Interface Guidelines

System	HSI Guidelines Referenced	HSI Guidelines Cited	Local Control Panel Guidelines Referenced	Local Control Panel Guidelines Cited
RCS	Yes	Yes	Yes	Yes
CVS	Yes	No	Yes	No
VAS	No	No	No	No
FWS	No	No	Yes	No
VFS	No	No	Yes	Yes
ZOS	No	No	Yes	Yes

Table 19: Implementation of Human System Interface Guidelines

System	HSI Guidelines Referenced	HSI Guidelines Cited	Local Control Panel Guidelines Referenced	Local Control Panel Guidelines Cited
CCS	No	No	Yes	Yes
PSS	No	No	Yes	Yes
PMS	No	No	Yes	Yes
SGS	No	No	No	No

389 Subsequent to above assessment, I received the Fuel Handling System (FHS) SSD (Ref. 111). The sections on controls and on the HMI include a number of requirements related to HF; however it makes no mention of the HF guidelines documents.

Integration to Training

390 Westinghouse has documented the incorporation of *HFE* into the development of the AP1000 plant training programs (Ref. 112). The document provides a summary of the HF activities and outputs, and then links those outputs through to the training provision, with a full audit trail. I have not assessed the document for accuracy or completeness, but from a HFI perspective, it appears to be an asset to those undertaking the training needs analysis.

Integration with other Technical Disciplines

391 I have been unable to locate any formal processes or systems in place to facilitate the integration of HF with other technical disciplines. The HFEPP states that it is essentially part of the role of *HFE* lead to facilitate the necessary interactions on an informal basis. I would expect more formal arrangements to be developed as part of any HFIP for UK construction of an AP1000.

> ***AF-AP1000-HF-44*** *- The licensee shall provide formal arrangements for HFI with other technical disciplines as part of their HFIP for UK construction of and AP1000.*

4.5.3 Management, Organisation and SQEP

392 HF is placed within the C&I function, and is focused on HSI design for the operational control centres. I consider that the placement of the team may limit their ability to fully integrate HF; particularly into the wider safety analysis function. In terms of team competency it is clear that the Westinghouse team are selected on the basis of formal HF qualification and experience, however there does not appear to be a requirement for PSA knowledge, and their Westinghouse training does not mandate wider safety analysis training. The HRA analysts are selected from a wide background, with no specific qualification requirement. There is an in-house peer review and technical mentor programme, but no HF training requirement.

> ***AF-AP1000-HF-31*** *- The licensee shall develop and submit a HFIP for UK AP1000 construction.*

4.5.4 Management of Risks, Issues, Assumptions and Uncertainties

393 The HFEPP highlights use of 'HFE Design Issues Tracking System', which appears to have the component features expected of such a system for issue management. I also note that the tracking system is not limited to HMI issues and does incorporate issues raised relating to PSA, maintainability, procedures, training, and work organisation etc. I was however surprised at the small number of items contained within the system for a project the size and significance as the AP1000 design (56 at the time of assessment); this calls into question the extent to which the system was used. I was unable to find any specific treatment of assumptions and uncertainties.

> ***AF-AP1000-HF-11*** *- The licensee shall develop, maintain and substantiate the HF assumptions as the safety case develops.*

4.5.5 Standards Applied and Relevant Good Practice

394 I briefly considered the HF standards base in my GDA Step 3 assessment (Ref. 6 refers) and later requested a comparability assessment between the standards applied by Westinghouse and recognised good (European) practice. Westinghouse specifically considered the requirements of NUREG-0700 (Ref. 10) in their design guidelines (along with other guidance and information from their previous experience); hence I have compared that with what I consider recognised good practice in Europe; as cited in my HFI TAG (Table 20 refers):

Table 20: Human Factors (European) Good Practice Comparison with Westinghouse Standards and Guidance

European Recognised Good Practice	Assessment of Westinghouse Compliance
BS EN ISO 11064 Ergonomic Design of Control Centres (Ref. 95)	This standard is much wider in scope than NUREG-0700 (Ref. 10), and places requirements on the design process that do not have equivalents in NUREG -0700 (Ref. 10). The standard is also process based, and there are differences in requirements at the technical level (relating to the acoustic environment for example). I judge that the Westinghouse 'core' programme is essentially compliant with the general principles and considerations of part 1 of the ISO standard, but in general falls short; largely due to differences in scope and approach.
ISO 6385 Ergonomic Principles in the Design of Work Systems (Ref. 96)	For the 'core' programme only, Westinghouse meet the majority of the requirements of this standard, and the areas that I consider they fall short are out of scope for GDA.

Table 20: Human Factors (European) Good Practice Comparison with Westinghouse Standards and Guidance

European Recognised Good Practice	Assessment of Westinghouse Compliance
ISO 13407 (now ISO 9241-210;2010) Human Centred Design for Interactive Systems (Ref. 97)	The Westinghouse 'core' programme meets the majority of this standard for human-centred design, with only minor shortfalls noted relating to the lack of a target audience description and issues regarding the concept of operation.
ISO TR 18529 Human Centred Lifecycle Process Descriptions (Ref. 98)	The Westinghouse core programme largely compliant; issues as previous.

395 The standards above are confined to HFI to the design process. I have considered the suitability of the 'standards' applied to the HRA as part of my Work Stream 2 programme.

4.5.5.1 Westinghouse Comparability Assessment

396 At my request Westinghouse undertook a benchmark of their (design) standards against UK expectations (SAPs) and recognised British and International good practice. Westinghouse claim that the UK SAPs are broadly comparable with NUREG-0711, and that the combination of NUREG-0711 (Ref. 54) and NUREG 0700 (Ref. 10) offer a broad comparison with IEC 60964 Nuclear Power Plant Control Rooms – Design.

397 The UK safety case states *"NUREG-0711 is considered to be equivalent to the HSE SAPs for Nuclear Facilities, in that it provides detailed Human Factors guidance for the U.S. as the HSE does for the UK."* It concludes *"NUREG 0711 is a regulator's guide which can be considered in the same light as the UK Safety Assessment Principles for nuclear facilities and is comparable to the UK SAP TAG on Human Factors in terms of providing appropriate Human Factors guidance for operators. The content of NUREG 0711 is broadly compatible with IEC 60964, IEC 61839, and IEC 1771."* I consider this a misunderstanding by Westinghouse, in that the SAPs are not detailed human factors guidance. I also neither consider the SAPs are aligned to NUREG-0711 (Ref. 54), nor would I be seeking this; the standards applied to the safety analysis and design should be at a much lower level and aim to deliver the intention of the SAPs as an outcome. I did however briefly compare the SAPs against NUREG-0711 (Ref. 54), with the conclusion that the criteria are not explicitly aligned largely due to scope and emphasis issues.

398 I assessed the comparability of BS IEC 60964 (Ref. 94) with the combination of NUREG 0700 (Ref. 10) and NUREG 0711 (Ref. 54), and the Westinghouse claim of comparability was largely upheld. Given that BS IEC 60964 (Ref. 94) is the most defensible standard in terms of good practice, then it is quite possible that appropriate use of NUREGs 0700 (Ref. 10) and 0711 (Ref. 54) would produce a control room that incorporates recognised good practice. However, it must be noted that the combination of the two NUREGs would be required to achieve equivalence. For example BS IEC 60964 (Ref. 94) requires a job analysis. Job design appears in NUREG 0711 (Ref. 54), linked to task analysis, and playing a broadly comparable role (though linked to validation) but the topic does not appear in NUREG 0700 (Ref. 10). It should be noted that I did not undertake a detailed line by line assessment of the Westinghouse application of NUREGs 0700 (Ref. 10) and 0711 (Ref. 54) to consider whether the application can be benchmarked against BS IEC 60964 (Ref. 94).

399 I also considered the currency of the standards applied and their updating, as part of the ALARP position. It appears that Westinghouse rely on the NRC updating of their NUREGs, and do not have a process within HF for routinely monitoring international developments as part of their ALARP decision making.

> ***AF-AP1000-HF-45*** *- The licensee shall apply relevant good practice and modern HF standards and guidance to the continuing design and development of the UK AP1000 and its safety submissions fully reflecting the work required in response to the GDA Step 4 Assessment Findings. The standards and guidance applied should be justified as part of the continuing safety submissions.*

I sampled the implementation of a recognised good practice standard to the design via the Alarm Presentation System (APS) specification. The recognised good practice in this area is the application of the Engineering Equipment and Materials Users' Association (EEMUA) guidelines 191 (Ref. 142). Within the Westinghouse HSI guidelines there are 57 mandatory guidelines for alarms; these cover expected aspects of alarm design. Additionally the APS functional requirements specification also includes requirements derived directly from the EEMUA guidelines.

4.5.5.2 Application of Operational Experience Review (OER) and Feedback (OEF)

400 The HFEPP states that OER was used to determine the functional requirements of the MCR, the WPIS, display design, and the HSI design guidelines, but I have not been able to trace this through Westinghouse's process. I note that there were five issues identified for input to the design issue tracking system relating to: actuation cycles for the Emergency Core Cooling System (ECCS) and reactor protection; operator-selectable alarms; soft controls, including touch screens (two issues) and feed water automation. This seems a very small number for the size of design project and in my opinion represents a missed opportunity. "The Incorporation of Human Factors Engineering into the Development of AP1000 Plant Procedures" (Ref. 92) also reviewed the material in the OER for lessons related to procedures and to design. I consider that this was effective use of the OER; with 41 issues identified and addressed. In some cases, I would have hoped to see that an issue was being tracked to resolution, but that has not been possible. "Human Factors Engineering Analysis to Support Technical Support Center and Emergency Operations Facility Design" (Ref. 93) included an additional OEF exercise for the design of the TSC. It identified 84 issues. Most of these were assigned as the utility's responsibility, but there does seem to have been a genuine effort to determine design aspects where possible. Again, it is not clear how these are tracked to closure.

401 I also note that Westinghouse has commenced a lessons learned programme. I have not assessed its application by the HF team, or for HF issues, although it does appear to offer potential in terms of performance indicators.

4.5.6 Conclusions

402 In general I judge that Westinghouse has evidence of a *HFE* programme of work; but it is limited to a HF engineering scope of work, which is in itself limited by Westinghouse's programme and resource split into core, adjunct and peripheral elements. This split is risk based and does not take explicit account of complexity and novelty; and in my opinion this does not necessarily result in an ALARP position. 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.

403 I judge that my observations in this area are most appropriately taken forward via Assessment Findings (**AF-AP1000-HF-31** to **AF-AP1000-HF-45** inclusive) to be incorporated into the HFIP for any UK construction of an AP1000.

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

404 In the UK HF safety case (Ref. 35) Westinghouse make the overriding claim that: *"The role of the operators in ensuring nuclear safety in the AP1000 has been minimised"* (Claim 1.0 Ref. 35).

405 This is supported by Claim 1.1 which states that *"The operators ensure nuclear safety throughout all plant modes of operation through proper plant procedure execution and compliance, including verification of proper automated system operation and manual intervention when needed"* (Claim 1.1 Ref. 35)

406 Two arguments are provided to support Claim 1.1 which have direct relevance to the Work Stream 2 assessment:

"The operating philosophy of the MCR operator is to monitor and control the plant safely under normal, abnormal and emergency conditions…… (Argument 1 Ref. 35); and

"It is important to the operating philosophy of the AP1000 that operator tasks are performed according to a procedure. A complete set of procedures has been developed for all plant operating modes and for activities including maintenance, normal operation, abnormal operation and emergencies……(Argument 2 Ref. 35).

407 Further claims (and their associated arguments) relating to the identification of operator and maintainer errors, and the means by which the design of the AP1000 ensures that the *"contribution to risk associated with their occurrence will be ALARP"* (Claims 1.2.1, 1.2.2 and 1.2.3 Ref. 35) are also relevant to Work Stream 5.

408 This section explores the robustness of these claims and arguments against the evidence presented. The evidence base considered is largely a myriad of references from the HF safety case.

4.6.1 Allocation of Function

409 These findings relate to item (1) from the methodology and scope presented in Section 2.2.9.1.

410 This section provides an assessment of the functional allocation process, and the adequacy of the implementation of the approach to functional allocation, via an examination of a sample of six of the main critical safety sub-functions.

4.6.1.1 Westinghouse Allocation of Function Methodology

Baseline Assessments

411 The AoF methodology that has been adopted by Westinghouse is described in Ref. 113. The earlier revision of this document was limited to AoF considerations for AP600 and it was understood that the revised version (Ref. 113) was primarily intended to extend the functional analysis to AP1000. However, whilst Ref. 113 does mention AP1000 in its title,

I note that after the title page and the preliminary pages, there are no specific references to AP1000 throughout the main body of the document.

412 The approach taken by Westinghouse to determine the appropriate functional allocations for AP1000 appears to have two strands. First, an initial set of functional allocations based upon past experience with other plants was used as a baseline functional allocation. This defined six Critical Safety Functions (CSFs), which were then subdivided into 39 different sub-functions. Westinghouse then undertook an assessment of the adequacy of the functional allocations for each of these sub-functions, by applying a systematic AoF algorithm, based upon that proposed in Ref. 115. Where necessary, the functional allocations were then amended to define the final functional allocations.

413 The baseline functional allocation was developed from the functional allocations that were adopted for the Westinghouse PWR reference plant, which is taken as the generic design for currently licensed Westinghouse PWRs. The six CSFs identified in the ERGs for AP600 were broken down into a comprehensive set of the main sub-functions, and the functional allocations that were adopted for these sub-functions then formed the baseline functional allocation. It was then argued by Westinghouse that the CSFs for AP600 would be similar to those used in the reference plant and so the same baseline AoF was then adopted for AP600.

414 Although AP600 was only a conceptual design, the same baseline functional allocation has now been used to underpin the AP1000 AoF. However, the existing operational PWRs, which are based on the original reference plant design, have now been operational for several years, during which time there have been substantial changes in interface technology and computer-based operator support. The impact of these differences upon the ERGs is considered in Ref. 117. Therefore I consider that it would be appropriate to modify this baseline to reflect such technological changes. I note that whilst Ref. 113 purported to assess both AP600 and AP1000, I found little evidence that the underlying baseline functional allocation reflected any of the interface changes between these two designs. Indeed, it appeared to be based upon operational experience gained on plants that have markedly different interface requirements from AP1000.

415 Therefore I conclude that the baseline functional allocation was not an ideal point from which to start the functional assessments for AP1000.

Westinghouse Detailed Allocation of Function Assessment Method

416 The second part of the Westinghouse methodology used the baseline functional allocations as a starting point from which to make more considered and in-depth assessments of the proposed allocations. Therefore Westinghouse proposed to identify any inadequacies in the baseline allocations, such that they could subsequently be modified by this more detailed assessment. Further summary information on the Westinghouse method is provided in Ref. 77.

417 The first of the identified inadequacies was consideration of the impact of automation upon situational awareness. This is important in determining whether a particular sub-function should be automated, as it is recognised that operators can rely too much upon automated processes, to the detriment of their normal monitoring. In the worst cases, this means that automation can lead to operators placing too much reliance upon alarms to notify them of potential problems, such that their situational awareness becomes degraded, or even non-existent, for some sub-functions. In such situations, alarms could be perceived as completely unexpected events that must then be diagnosed, rather than being seen in the context of overall plant performance, in which operator intervention can

often prove effective in preventing the edges of the normal operating envelope from being reached.

418 The second issue was the lack of any specific consideration within the decision algorithms of situations where control was shared between the system and an operator (although I note there was limited guidance for such situations in Section 3.1.3.1 of Ref. 113). For such tasks, it is important to ensure that the level of operator support that is provided is commensurate with and appropriate for the particular application; such that workload is kept within reasonable levels, without limiting the operators' situational awareness.

419 I judge that providing that this methodology was applied consistently and effectively, the functional allocations that were developed would comply with SAP EHF.2. However, I also recognise that the criteria that were provided for assessors are generally subjective and many rely upon HF judgements that require a clear understanding of the underlying issues. Therefore, the effectiveness of this approach also depends to a large extent upon the way that these criteria are interpreted by the person making the AoF decisions. I considered that the assessment of a sample of the functional allocation decisions would provide an effective check that their decisions were realistic and did not contradict the balance of evidence; and this is provided below.

4.6.1.2 Assessment of a Sample of Six Functional Allocations

Main Feedwater

420 A summary description of this system is provided in Ref. 77.

421 The Westinghouse AoF analysis for the main feedwater sub-function concluded that the required tasks imposed a relatively high workload that could lead to overload if they were allocated to human operators. Therefore, Westinghouse proposed to use automatic flow controllers for both the start-up and the main feedflow. When these are set to automatic control, the flow controllers should ensure that the SGs remain within the accepted limits throughout the power range, and when both controllers are operating automatically, the change between start-up and main feed systems should also be managed effectively without further operator intervention. It was also concluded that an operator would have sufficient indications of feedflow and SG levels to monitor feedflow effectively whilst undertaking other tasks.

422 The Westinghouse walk-through assessment confirmed that feedwater control should be an automated function and the design of the automated flow controllers supported the tasks that were required. In particular, the flow controller interfaces should enable a single operator to set all the valves to maintain the SG levels within their acceptable limits, without any unreasonable additional workload. The monitoring requirements would then not impose any unreasonable additional workload; hence it would not be necessary to allocate an additional operator to this function, even during power changes. Once all of these flow controllers have been set to automatic control, the operators will have clear indications that can be used to monitor the situation, however because the flow controllers will also manage the valve position adjustments, such monitoring will not be very onerous. Therefore although feedflow will generally be controlled automatically, the other interfaces should provide the operators with clear awareness of the SG levels and the associated feed and steam flows.

423 In the event of the failure of one or more of the flow controllers, auditory alarms would warn the operator before a critical SG level is reached and this would provide sufficient time to select manual control and take appropriate corrective action. The interfaces for

the feedwater controllers conform to a standard design that is simple to use and therefore in the event that an operator had to operate these valves manually, this should not present any difficulties due to a lack of familiarity.

424 Whilst this automated flow control will inevitably reduce the operator's awareness of the actual flow rates and valve positions during normal operations, the operators will be able to maintain good awareness of the steam generator levels by monitoring these on the Reactor Overview screen of the WPIS, backed up with trend displays if necessary. Therefore, by placing less reliance upon the position of the flow controllers, the operators will find it easier to maintain their awareness of the SG levels; which are the parameters that are of most concern.

425 The main feedwater function is one that should be automated, and I consider that the arrangements for this automation are likely to ensure that the operator maintains good situational awareness. I have no issues with the Westinghouse analysis and AoF decision in this case.

Normal Residual Heat Removal System

426 A summary description of this system is provided in Ref. 77.

427 If the RNS is to be operated manually, an operator must first initiate flow through the RNS circuits at a desired flow rate, and then open the bypass valves to divert some of this flow from the heat exchangers. To do this, the operator would (probably) monitor the trend displays of the RNS temperatures, and adjust the flows through the RNS and the heat exchangers to try to keep the temperatures falling at a rate close to the optimum. As the input temperatures at the heat exchangers decrease, it will become necessary to adjust the relative flows, which imposes a relatively high workload at a time when there are also many other tasks to be undertaken. These workload concerns were identified by Westinghouse as a reason for automating the RNS system. Automation would also provide some protection against a lack of vigilance, which could mean that the operator failed to adjust the flows through the heat exchangers sufficiently as the cool down progressed. However, the dynamics of heat exchangers are such that this is more likely to result in a slowdown of the cool down which would have an economic impact, rather than exceeding the safe cool down rates. This is because the flow has to be increased as the temperature differential at a heat exchanger decreases.

428 However, there were also some advantages identified for manually controlling these valves, as manual control would provide an opportunity to vary the cool down rate whilst maintaining at the maximum rate. Faced with this ambiguity about the AoF for this sub function, Westinghouse decided to provide flow controllers for both sets of valves, whilst still requiring the operators to initiate RNS flow and to set the overall RNS flow rate (RNS-V006A and B) and the target cool down rate. The former being set by the controllers for RNS-V006A and B, whilst the cool down rate (RNS-V008A and B) was automated.

429 It was evident that if the RNS was operated under manual control, valve adjustments would be relatively frequent, and during the early stages of RNS cooling, there could be some difficulty in predicting the impact on the cool down rate of particular rates of flow through the heat exchangers and the bypass lines. There was also a possibility that a cool down period might be extended because an operator was not monitoring the effects of a cool down sufficiently closely. It was considered that the flow controllers to be provided would do much to eliminate these difficulties.

430 However, there were also advantages to allowing the operators to set the flow rates and cool down rates. The associated interfaces for the RNS were considered to make the initiation of RNS cooling a straightforward task, and to ensure that a cool down could be

effectively monitored and controlled. Therefore, by providing a combination of automation for fine control together with manual intervention to set the flow rates and cool down rates, the functional allocations implemented by Westinghouse for the RNS met the requirements identified in their AoF analysis.

431 The way in which the RNS has been automated is likely to help to minimise workload and vigilance problems, whilst providing operators with some direct control over the flow rates and cool down rates. By providing this operator control, the operators still maintain their awareness of the progress of the cool down. I have no issues of note regarding the Westinghouse analysis and AoF in this case.

Pressurizer Auxiliary Spray

432 A summary description of this system is provided in Ref. 77.

433 Using the auxiliary pressuriser spray is a relatively rare action that should only be undertaken following confirmation of the failure of the normal pressuriser spray. Once a decision has been taken to use the auxiliary pressuriser spray, the preparations are straightforward tasks that would not impose a significant workload and hence there would be no advantage in automation.

434 Once one of these valves has been opened, the flow through it cannot be controlled; hence the operator only has to monitor the depressurisation periodically as it progresses. Typically, the depressurisation would continue until a specific reactor pressure or pressuriser level had been attained, and in some cases this would be done in predetermined stages. It is also necessary to terminate a depressurisation if the sub-cooling margin is reduced too much. All these parameters can be monitored easily and alarms are likely to provide additional warning if critical values are being approached. In particular, operator-set alarms would assist the operators if it was decided to depressurise in stages. Therefore, the monitoring requirements should not impose any undue workload. Similarly, the termination of the spray is also a simple task. Therefore, it is considered that this is a task should be allocated to an operator.

435 In view of the low frequency of this task requirement and the simplicity of the actions I consider that automated control of the pressuriser auxiliary spray is unnecessary. Manual control of this function will involve relatively little workload for the operators. I have no issues with the AoF proposed by Westinghouse in this case.

Containment Make Up

436 After a substantial accident some water within the containment will collect in the sumps which could then be re-circulated. However there is a risk of leakage at one of the containment penetrations, which would result in a loss of inventory.

437 If such losses continue it would eventually become necessary to add more water from outside containment. Therefore, external to containment there are two manually operated isolation valves in the safety related piping to attach an alternative water source. Valves at these points can then be opened to deliver water into containment via the RNS.

438 Before this approach can be used, it will be necessary to provide a water source close to the valves. This water could come from a bowser or another source; hence temporary hoses would be used to transport water from this source to the site of the valves. There are several potential sources for this additional water and the selection of the most appropriate source will depend upon the prevailing circumstances. Therefore, the connection of hoses between the selected source and the valves will be a manually intensive task. However, it is postulated that even in the most severe situation such additional cooling will not be required within the first 72 hours of an event. By that time

there will be sufficient resources available for the task. Given these timescales and the low workloads that would be required to manually open these two valves, Westinghouse considered that this task should not be automated.

439 There is ample time available to connect an alternative source of water outside the containment, and providing that the isolation valves are clearly labelled, there is little risk of an incorrect connection being made. It will also be important for an operator to check that there is no leakage when the valves are opened. Therefore, it is considered that these valves should be manually operated rather than operated remotely.

440 Once flow has been established it is anticipated that the valves will be locked in an open position. Therefore, it will not be necessary to monitor the position of these valves directly from the MCR or the Remote Shutdown Room (RSR).

441 If inventory losses occurred in the vicinity of these valves it may be necessary for the operators to don appropriate radiological protection equipment before undertaking the tasks. However, whilst this will increase the time required, the workload should still be within acceptable limits and as the event frequency is so low, it is not considered necessary on ALARP grounds to automate these valves. I have no issues with the Westinghouse analysis and resulting AoF in this case.

Chemical and Volume Control System Boration

442 A summary description of this system is provided in Ref. 77.

443 In the event that there is a major leak in the RCS, it will be necessary to provide additional cooling as rapidly as possible. Therefore, Westinghouse considered it necessary to automate the initiation of alternative cooling from the CMT to meet their design requirements of reliance upon a passive system (such as the CMT). As well as automating the CMT initiation, Westinghouse proposed that the same signal should initiate all the associated CVS isolations.

444 In the event that the cooling could be provided directly from the CVS, the nature of the operations required becomes more varied and more dependent upon other factors. For instance, if the CMT has already actuated, then it may be necessary to close the CMT actuation valve. Westinghouse considered that the human operators can play a valuable role in determining how to align the CVS and hence they decided not to automate these tasks. However, Westinghouse noted that the desirable range for the pressuriser level in this situation was different from that during normal CVS operations; hence they decided to automatically set the CVS flow controllers to use the LO5 and LO6 set-points following a trip situation.

445 In the event that the pressuriser level falls sufficiently to require an injection of borated water from the CMT, it will be important to ensure that the CMT actuation is initiated rapidly and correctly, which also requires that the CVS is accurately isolated. Therefore, automating these steps provides confidence that they will be undertaken rapidly and correctly, without undue workload on the operators at a busy time.

446 However, in the event that there is an anticipated transient without scram or a relatively small break in the RCS, it becomes more important to have increased operator involvement. Therefore, it is considered appropriate to retain these as manual tasks.

447 If the CVS is being used to prevent the requirement for ADS cooling, the operator could manually set the CVS flow controllers to operate in manual mode, using different minimum and maximum pressuriser levels to those normally adopted. However, there is the potential that under the relatively stressful post-trip conditions, the operators could fail to

remember that these levels should be reset, and hence the decision to automatically reset these levels after a trip signal is also considered to be helpful to the operators.

448 There are arguments both for automation and for manual control of the CVS. However, I consider that Westinghouse's allocations of the constituent tasks between humans and automated systems provides a good balance, which should provide the operators with support for tasks that would otherwise increase their workload, whilst also providing flexibility in the approach that they decide to take when there is not such an immediate need for additional cooling. The automatic resetting of the pressuriser level set-points is a good way to avoid potential errors that could occur in the stressful time following a trip. I have no issues of note regarding the Westinghouse analysis and AoF in this case.

Circulating Water

449 The circulating water system does not require regular monitoring; once it has been set up on start-up, it will only be necessary to conduct any operations on this system if a pump stops. This could occur because of an unexpected pump fault, in which case the standby pump must be aligned and then started, or because of a loss of off-site power, in which case the pump must be restarted once power is available. In either situation there will be no urgency to reinstate the circulating water.

450 Therefore, as there is only an infrequent requirement to restart a circulating water pump, and as there is a wide time window available for doing this, Westinghouse determined that due to the cost of automation and the added complexity that it added, the appropriate pump should be started manually from the MCR rather than the being automatically re-aligned and started upon the failure of a circulating water pump.

451 If a circulating water pump fails, an alarm will be raised in the MCR, and the valves can then be re-aligned and a pump started from the MCR via up pop-up displays. If this occurs during normal operations, the standby pump can be started very quickly, as described in AOP 320.

452 In the event that there is a loss of off-site power, restoration of circulating water could be seen as a low priority, and an alarm for the failure of a circulating water pump could easily be missed. However, the procedure for dealing with a loss of off-site power will direct the operators to restart a circulating water pump, which should act as an adequate cue to prompt this action.

453 Either of these events will be relatively infrequent and there will be sufficient time in which to restore circulating water. Therefore, this task need not be automated, and restarting the pump manually will not greatly increase the operator's workload.

454 I consider that this is a very straightforward task and there would be little benefit in automating it. Therefore, I have no issues regarding the Westinghouse analysis and AOF in this case.

4.6.1.3 Conclusions

455 The baseline functional allocations used by Westinghouse were based upon a relatively dated generic design that had not been adequately updated to reflect developments in interface technology. Although the baseline functional allocations were not an ideal starting point for determining the functional assessments, I consider that the second stage of the methodology was reasonably comprehensive and in compliance with current HF guidance on AoF criteria. However, I note the omission of any formal consideration of the impact of automation on situational awareness and that there was no specific mention

within the decision algorithms of situations where control was shared between the system and an operator, though such situations appear to be relatively rare in NPP applications.

456 In summary, I judge that the systematic AoF algorithms provided a good basis upon which to determine functional allocations and to ensure that these comply with the requirements of SAP EHF.2, providing that they are applied appropriately and consistently.

457 Regarding the sample of six functional allocations that I assessed, I judged that the functional allocations and the underlying reasoning that was proposed by Westinghouse were appropriate. Also, the implementation of these sub-functions complied with good HF guidance.

4.6.2 Task Analysis

458 These findings relate to item (2) from the methodology and scope presented in Section 2.2.9.1. I focused my assessment on the scope of issues considered by the task analysis; the adequacy of the task analysis processes and the presentation of the task analysis data.

459 Westinghouse offer 3 formal task analyses; the FBTA; OSA-1 focussing on identification of indications, controls and alarms to support task performance, and OSA-2 which was focused on operator and crew workload, detailed analysis of task performance requirements for risk-important tasks and MTIS task analysis.

4.6.2.1 Function Based Task Analysis

460 Westinghouse claim that the FBTA process examines the tasks required for safe operation of AP1000 in a way that is both systematic and comprehensive, and which should provide confidence that the interfaces modified and developed from the FBTAs are complete. This claim is restated in Ref. 118, which states that the results from the FBTA will feed into the design of the Human–System Interfaces (HSIs) to *"Obtain a completeness check on the availability of needed indications, parameters, and controls. This includes indications and controls needed for supervisory control of automated systems and manual override"*.

461 The FBTAs started from the system functional goals, and presents the analysis data in a series of tables. Within each table all the tasks required for the main AP1000 systems were re-described in further detail. This involved first defining all the constituent sub-functions and then identifying their associated goals. From these analyses, Westinghouse defined the task requirements that were needed to enable an operator to achieve these goals. These were specified in terms of the specific decisions or actions required and the supporting controls and displays to be provided within the MCR.

462 I examined these tables in some detail and I consider that they provide sufficient information to enable Westinghouse to ensure that the function-based displays comply with all of the aims of the FBTA. Westinghouse has specified that the FBTA is intended to support the design of the function-based displays only; however I note that the information within the FBTA report could also be used effectively for the design of other software or hardware interfaces, both within the MCR and local to plant. The data could also be used to support the design of operational procedures and other documentation and Refs. 92 and 112 indicate that Westinghouse have used the FBTA in this way.

463 It is not possible to confirm how much of the FBTA data was applied by Westinghouse, but I note that the data generated meets the criteria that I highlighted in Section 2.2.9.1,

regarding the expected scope of task analysis to support the design of operational interfaces.

464 With regard to the adequacy of the FBTA, I consider that the approach used was adequate for this application, and based on the content of the analyses reviewed, it is clear that the analysts involved were competent and have provided a thorough analysis.

465 The FBTA report did not provide any detail about the source of the information that was used. Therefore, I felt that it did not meet my criterion for explaining data sources. However, the data was extensive and my review of the tables in the FBTA report provides me with some confidence that the data that was generated for the instrumentation requirements was reasonably complete. It was also evident that sufficient detail was provided about the task requirements and the display details, to ensure that the resulting individual display and control elements could be accurately represented on appropriate display formats.

466 I took a sample of two systems and assessed how the display formats for those systems comply with the data provided in the FBTA. For this purpose, I was limited to the sets of high level (Level 2) displays for the specific systems. In this case, all of the MCR-operated displays and controls from the two systems were accurately presented on the display formats; hence the FBTA tables did provide an effective way to check the completeness and accuracy of the controls and displays that are used in the MCR. However, I note that although locally operated components were identified in the FBTA, none of these were shown as static representations on the formats. I note this omission, although it is possible that information does appear elsewhere on more detailed displays that I was not able to examine. Finally, I note that although alarms are mentioned in the FBTA, I was unable to check whether the alarms identified in my sample were included in any alarm lists, as the alarm database definition tables were neither developed nor available at the time of my assessment.

467 In summary, the FBTA derives from a hierarchical systems functional analysis of the plant, and therefore the scope should be relatively complete. I note minor issues that the sources of data used for the analyses were not explained, and I have not been able to determine whether information from the analyses has been used to modify the design of user interfaces. However these minor points to not undermine compliance with the relevant SAP (EHF.5).

4.6.2.2 Operational Sequence Analysis 1

468 OSA-1 examined the operational requirements of ten substantive scenarios that were listed in the DCD (Ref. 64). Four further scenarios were subsequently added. Westinghouse claim that the OSA-1 assessment: provides findings and recommendations for use with display design for AP1000; compiles the inventory and frequency of use for alarms, controls, components, and parameters required to perform the scenarios identified in the DCD and identifies performance time constraints on operator actions, which may require particular display designs.

469 I consider that the set of scenarios assessed in OSA-1 were representative of the key MCR-based tasks for AP1000. Also, the analysis does provide a good opportunity for assessing risk important tasks, which should support the HRA.

470 I was not able to examine the underlying OSA-1 database, hence my only source of information with which to assess these analyses directly were the ‘road maps’ (or scenario descriptions) and Operational Sequence Diagrams (OSDs) that were presented as

Appendix A of the OSA-1 Report (Ref. 119). Without the underlying database, I had to rely upon the data interpretations that were summarised by Westinghouse in the OSA-1 report and elsewhere. This meant that I was not able to check these against the raw data. Within Appendix B of the OSA-1 Report Westinghouse listed 23 findings from the scenarios and a further two for specific risk important tasks. All of these findings appeared to be reasonable, but generally I considered them to be relatively straightforward issues that could have been identified by other less resource-intensive means. For example the statement that *"Many parameters must be checked periodically during procedure execution to ensure correct trending"* was not surprising for a complex system such as AP1000. Similarly, the requirement to monitor shutdown margins could have been anticipated without having to populate such a large task database.

471 I note that there are a few examples of OSA-1 data being used to improve interface designs (Appendix B of the OSA-1 report refers); in the absence of a comprehensive list of how OSA 1 material has influenced the design I can only judge that its impact has been minimal. I note that Westinghouse aimed to obtain temporal information and develop an inventory of required interface components, however these aspects do not appear in the summary report.

472 I consider that the set of scenarios and the safety significant actions were both representative and sufficiently comprehensive. The methodology could have provided insights about safety important tasks, but this opportunity was not taken, and uncertainties surrounding the data sources mean that I could not directly make a judgement about their adequacy. I note the very limited number and simplicity of issues that were raised and the lack of underlying explanation and insight that was provided. In summary I consider it unlikely that the OSA-1 analyses have generated sufficient understanding of the analysed tasks or their interface requirements to support a sufficient insight into the risk presented by the analysed tasks. This also carries the consequential risk that engineered design provisions have been overlooked or are insufficient.

> ***AF-AP1000-HF-46*** *- The licensee shall review and provide further analysis relating to the scenarios of the Westinghouse Operational Sequence Analysis 1.*

4.6.2.3 Operational Sequence Analysis 2

473 OSA-2 was designed as a follow on to OSA-1, to evaluate the HSIs. The OSA-2 Implementation Plan (Ref. 120) indicates that the focus was on assessing:

- Completeness of available information. This analysis determines whether necessary information is available to the operator performing the task activities.
- Time to perform tasks. A set of performance time assumptions will be established and used to determine the time required for tasks to be completed. These assumptions will provide estimates of task performance times that can be compared to performance time requirements.
- Operator workload analysis – An evaluation of the effect of the HSI design and the task demands on operator workload.
- Operational crew staffing. Using the workload analysis to provide an indication of the adequacy of staffing assumptions.

474 OSA 2 adopted a risk informed approach to the selection of tasks for analysis, and included MTIS tasks associated with 38 components. The data for these tasks were

collected in a similar way to OSA-1 and hierarchical task analyses were then undertaken for each task.

475 It is clear from the summary report that Westinghouse focused very strongly on task times in the assessment. Times were originally to be estimated from times developed by the American Nuclear Society (ANS); however Westinghouse then analysed video footage of simulator trials and applied the average times calculated from these instead. The justification presented for this was that these were more appropriate as they better represented the use of the AP1000 MCR controls and displays. However, it is apparent that many of the revised times were shorter (than the ANS times); and in one case this meant that a time critical task was assessed to be achievable using the Westinghouse data, yet failed using the ANS data. Therefore, I consider that it would have been prudent to have taken the simulator data as validating the ANS timings, and then to have applied the more conservative ANS data. Horizontal, stepped timelines were produced for all the scenarios based on the average times for generic tasks from simulator trials. An assessment of a sample of the timelines indicated that they had been drawn accurately. The overall task times from these timelines were then used to determine the overall task times for the time-critical sequences.

476 For each of the tasks a *'workload'* assessment was undertaken by dividing the predicted time required into the time available and expressing the result as a percentage. I do not consider that this was a measure of workload, but is better defined as the potential *'utilisation factor'*. As such, this figure only provides an indication of the viability of completing a particular task within a prescribed time and does not provide any direct indication of the potential stress or cognitive difficulty likely to be experienced. As the predicted time required approaches the time available, the likelihood of failing to complete the task within the required time increases. It is difficult to define a criterion for an acceptable utilisation factor, because this depends upon the level of risk of non-completion that is deemed acceptable. To place this into context, I assessed Westinghouse's treatment of one specific task, which had a utilisation factor of 95%. Westinghouse used average times for the timelines and the workload calculations; hence a 95% utilisation factor means that only 50% of the operators attempting this task will complete it within 95% of the time available. Or in this particular case 50% of the operators will have a margin of three seconds or less in which to complete this task within the required time. However, in interpreting this situation, Westinghouse state in Ref. 87: *"Nevertheless, the operator workload in Task 4 is still considered to be acceptable, because a very short period of high workload, such as 95 percent workload over one minute in this case, is acceptable if the operator workload over an extended period of time (e.g., a shift) is within the ideal range (Kirwan and Ainsworth, …1992)"*.

477 If it was workload that was being measured, I would agree that a very short period of high workload would be relatively easy for operators to cope with and I would have found such a conclusion acceptable. However in this particular case the tight time margins are an issue. In any case Westinghouse has used an incorrect statistical interpretation of 'workload' data to justify this situation as being reasonable. Therefore, I consider that this interpretation shows that Westinghouse does not fully understand perceptual and mental workload concepts. I also note that Westinghouse consider that acceptable performance for time-critical tasks can be claimed when the average times are particularly close to the available times. I therefore consider that a prospective licensee will be required to undertake additional workload analysis.

> ***AF-AP1000-HF-47*** *– The licensee shall undertake workload analysis using recognised analytical techniques.*

478 As these were multi-person tasks, Westinghouse also tested their staffing proposals for the operational crews by looking at how these might be implemented during the scenarios that were examined. For emergency operations, Westinghouse made the assumption that, *"the MCR will be staffed by one Shift Technical Advisor (STA), one Senior Reactor Operator (SRO), and two Reactor Operators (ROs) (RO1 and RO2)"* (Ref. 87). This is the same staffing assumption that is used for the PRA (Ref. 67) and hence I consider that it provides a reasonable basis for the OSA-2 assessments. The assessments provided some verification for these staffing arrangements and provided realistic estimates of the times required to undertake the assessed tasks. However, a prospective licensee will be required to reconsider these analyses against a UK staffing structure should that be different to the Westinghouse proposals.

> ***AF-AP1000-HF-48*** *- The licensee shall review and re-analyse the Westinghouse operational sequence analyses 1 and 2 against their proposals for a UK staffing structure, should that differ from the Westinghouse proposals.*

479 The second part of OSA-2 assessed selected maintenance, test, inspection and surveillance (MTIS) tasks using Hierarchical Task Analysis (HTA), and the results are presented as a comprehensive set of HTA diagrams. I have not seen the database entries for these tasks and hence I can only rely upon the HTA diagrams presented in Appendix C of the OSA-2 Report to interpret the results.

480 I note that many of the tasks are re-described into a relatively large number of subtasks. I would not typically expect tasks to be broken down into more than six or seven subtasks, apart from some maintenance tasks where a large number of components must be disassembled or assembled to meet one goal. However I note that some operational tasks were re-described into as many as 23 subtasks, which can be symptomatic of the analyses having been developed almost entirely from procedural documentation; often directly structuring the HTA hierarchy from the structure of the procedures. This can result in task factors outside of the procedures not being captured by such an analysis. As a result I judge that this analysis of maintenance tasks appears to be of limited insight and use. As a result a prospective licensee should reconsider and supplement the analyses for MTIS tasks on a proportionate and targeted basis.

> ***AF-AP1000-HF-49*** *- The licensee shall review, reconsider and supplement the task analyses for MTIS tasks on a proportionate and targeted basis.*

481 I judge that the timeline analyses used appropriate methods but that the data source used for the generic times was optimistic. I do not consider that the workload assessments undertaken by Westinghouse allow conclusions to be drawn about mental workload. In addition, there is a strong potential for optimism in estimating task durations both in terms of the statistical processing of timeline data and in the derivation of observed simulator task timings that form the basis for estimations. I consider that the graphical form of presentation of the temporal information on the timelines and associated tabulations is acceptable, but the presentation of the results of each task assessment is somewhat limited in its utility.

4.6.2.4 Conclusions

482 It is clear that Westinghouse has undertaken a sequence of analytical work on tasks, and the scope of that work is broadly acceptable for a PCSR. However I consider that there are methodological, quality and application issues that challenge the Westinghouse claims

in this area. I consider that a prospective licensee should revisit these generic task analyses, in light of subsequent safety case and design developments post PCSR.

4.6.3 Workstation and Workplace Design

483 These findings relate to item (3) from the methodology and scope presented in Section 2.2.9.1.

4.6.3.1 Anthropometric Data

484 Westinghouse claims in the UK HF Safety Case (Ref. 35) that *"The AP1000 has been designed to physically accommodate the fifth percentile female to the ninety-fifth percentile male dimensions based on data collected for the U.S"*. Based upon an examination of data from Pheasant and Haslegrave (Ref. 22), Westinghouse then argues that *"These data are broadly comparable to similar data gathered for UK populations"*.

485 In its investigations of anthropometric data Westinghouse has examined four sources, and some of the most important human dimensions from these studies are summarised in Table 4.6-1 of Ref. 122. This table presents the 5th percentile female and 95th percentile male data for these dimensions from a Chinese standard, two US reports and a UK Defence Standard. These data are then summarised as Appendix A of the HSI Guidelines (Ref. 105) where they are stated to be data for the US population, although a detailed examination reveals that the Chinese data have generally been used for the 5th percentile females.

486 I note minor discrepancies between the data applied by Westinghouse and British data, with some falling outside the preferred range. However I judge that this will not significantly undermine the design or adversely impact human reliability. In my opinion, the most representative sources of anthropometric data for the British working population are Table 10.1 of Pheasant and Haslegrave (Ref. 22) and from Peebles and Norris (Ref. 123), and I consider that it would be more appropriate to apply the data from these two reports as the anthropometric source for the UK AP1000. I note that Westinghouse took account of footwear and corrected some of the dimensions accordingly. It should be clear within the relevant specifications that this has been done. A prospective licensee should review the anthropometric data source applied to the physical design of the AP1000 on a proportionate basis, against recognised UK data sets.

> ***AF-AP1000-HF-34*** *- The licensee shall review the anthropometric data source applied to physical design of the AP1000 on a proportionate basis, against recognised UK data sets. This should recognise reasonable estimates of the secular trend of the intended operating lifetime of the plant.*

487 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. 124, which suggests that the trend is currently at about 10 mm 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 Pheasant and Haslegrave (Ref. 22) was obtained in the mid eighties and hence once an AP1000 NPP is commissioned in the UK, some of the data could be over 30 years old. It must be noted that this does not just affect

estimates of length, but obesity trends will also impact the space requirements for personnel in future facilities.

488 I therefore consider that the workstations should be designed to meet the current user population, based upon reasonable estimates of the secular trend, and that this should be considered by a prospective licensee.

> ***AF-AP1000-HF-34*** *- The licensee shall justify the anthropometric data source applied to physical design of the AP1000 on a proportionate basis, against recognised UK data sets. This should recognise reasonable estimates of the secular trend of the intended operating lifetime of the plant.*

4.6.3.2 Main Control Room Layout

489 Westinghouse states that *"The operating environment, including the MCR, plant layout, and operating philosophy is based on established modern HF principles and practices"* (Ref. 17).

490 There are up to nine working positions provided within the MCR. Westinghouse proposes that the MCR will normally be operated by one SRO and two *RO*s. A STA may also be present, particularly during busy periods or emergencies, but there is no permanent requirement for an STA to be present. This arrangement is described in the Specifications for Control Rooms (Ref. 125) and in a plan of the MCR (Ref. 126). Drawings of the SRO and *RO* consoles are provided in Refs 127 and 128.

491 My assessment of the general approach by Westinghouse to satisfying HF issues in workstation arrangement is that Refs 125, 127, 128 and 129 provide assurance that HF has been systematically considered in the arrangement of the MCR. In addition Ref. 129 shows that representative utilities have been involved in a detailed review process which provides confidence in the practicality of the proposals.

4.6.3.3 Specific Workstation Design

<u>Distributed Control and Information System (DCIS) Workstations and Wall Panel Information System (WPIS)</u>

492 I have considered the physical design of the DCIS workstations, and while I note minor discrepancies between some of the physical dimensions and recognised standards in this area, I judge that overall the physical design will not compromise human performance.

493 I have reviewed the dimensions in Refs 127 and 128 and the anthropometric dimensions detailed in Ref. 22 to determine the acceptability of viewing angles and viewing distances. From the dimensions of the desk and screen shown in Ref. 127, I expect all users of the SRO and *RO* consoles to have a downward viewing angle to the centre of the screen. For a 95th percentile male, there will be a downward viewing angle of 30° to the centre of the screen and for a 5th percentile the angle would be 8°. I judge these viewing angles to be satisfactory.

494 The worst case viewing distances to the screen would be those for taller individuals. I have estimated that a male individual with 95th percentile sitting eye height, sitting centrally in front of a screen would have a viewing distance to the screen of 765 mm. However, the design of the workstation is meant to allow coincident reference to up to four screens, which are arranged horizontally on the desk. This means that the viewing

distances may exceed the maximum recommended viewing distances to other screens even for smaller individuals. However this can largely be accommodated by operators moving/leaning closer to the screen when inspecting parameters or manipulating components.

495 My subjective view from observations of screen usage during my simulator visit is that the WPIS displays are legible, but probably close to the acceptable limit. However, I have not been able to determine the actual legibility of the WPIS display, as I could not obtain accurate details of the text sizes that are to be displayed. However, I have calculated acceptable minimum text heights for the WPIS from various operating positions, using a formula from Van Cott and Kinkade (Ref. 130), which are shown as Table 3 in Ref. 77. These calculations are based upon recommendations from NUREG 0700 (Ref. 10) that the minimum text size should be defined as 15 minutes of arc. I also note that British Standards for office work recommend a minimum character size of 16 minutes of arc (Ref. 157). However, I consider that these are both conservative recommendations, as normal vision (or normal corrected vision) discriminates characters subtending 5 minutes of arc when a black on white contrast illuminated at 120Cd/sq.m is used. Therefore, I have also provided figures for 10 minutes of arc, as this is double the size that can be discriminated by persons with normal (or normal corrected) vision. Provided that there is good contrast and illumination, I consider that text at this size will be well within the legibility limits for most people. For unsaturated colours, 15 minutes of arc may well be necessary and user testing is desirable to establish the situation; hence this should be included in the V&V programme.

> ***AF-AP1000-HF-50*** *- The licensee shall specifically include the legibility (text sizes and saturated colour contrasts) of displays at the expected viewing angles and distances in the V&V programme, prior to final decisions being taken on screen angles and character/symbol sizes.*

496 I have also examined the plan of the WPIS display layout. My calculations suggest that there is an upwards viewing angle over the top of the workstation screens to view the WPIS. I have considered the sightlines to the WPIS displays and I conclude that from the expected working position, the base of the WPIS screen is not obscured by the top of the DCIS screen. I have calculated that the minimum eye point height where the DCIS screen would be an obstruction is 925mm; hence the expected operator population is accommodated.

497 I am generally satisfied with the physical arrangement and dimensions of the DCIS consoles, and this was supported by my observations at the simulator facility. However, the legibility of the displays at the expected viewing angles and distances should form part of the V&V programme, prior to final decisions being taken on screen angles and character/symbol sizes in the displayed information. This applies to the DCIS screens themselves and to the WPIS screens.

> ***AF-AP1000-HF-50*** *- The licensee shall specifically include the legibility (text sizes and saturated colour contrasts) of displays at the expected viewing angles and distances in the V&V programme, prior to final decisions being taken on screen angles and character/symbol sizes.*

Primary Dedicated Safety Panel (PDSP)

498 I judge that the switches that are provided on the horizontal desk section of the PDSP are within easy reach of all expected users.

499 Using UK anthropometric dimensions from Pheasant and Haslegrave (Ref. 22) I calculate that the viewing angles for seated operators at the PDSP are within an acceptable range, and that the sloping screen angle provided of 15° is appropriate. I do not consider that the screen is well placed for standing operations, but it would be acceptable for limited use from a standing position.

Secondary Dedicated Safety Panel (SDSP)

500 There are no issues regarding reach to the switch controls on the SDSP. The distance between the SDSP and the PDSP clearly prevents operation of the controls at both desks by the same person, but they are sufficiently close to allow reliable communications between operators using controls on the two desks.

Diverse Actuation System (DAS)

501 I have examined the dimensions of the DAS Panel and I consider that the controls and displays are positioned within the acceptable ranges for all potential users to be able to read the numeric displays accurately and to operate all the controls.

Remote Shutdown Workstation (RSW)

502 The RSW contains a console desk with two dual-headed DCIS workstations and a Local Area Network (LAN) workstation; a total of five screens. The room also contains the Remote Shutdown Workstation Panel (RSWP), which can be operated from in front of the RSW. The RSWP has a sloping back panel for the manual operation of switches.

503 The console dimensions related to seated operation are the same as those provided for the MCR RO/SRO workstations (Refs 129 and 158). The RSWP design dimensions related to seated operation are the same as those provided for the SDSP. From Ref. 159 it is concluded that there should be no issues regarding the reach of controls; they are within reach and can be manipulated by the expected, smallest workers, generally from a standing position. The displays are visible and legible from the expected working position.

504 A gap of 1,016 mm is provided at the rear of the RSW console with more space provided behind the RSWP. I consider these dimensions marginally sufficient for any maintenance related activities to be conducted in relation to the console and panel, provided that lifting above 10kg and test equipment does not need to be taken into the area. However, access panels should preferably be lift-off and local maintenance lighting will be required.

> ***AF-AP1000-HF-51*** *- The licensee shall consider whether access panels on the RSWP should be 'lift off', and ensure that local maintenance lighting is provided.*

Other Control Rooms

505 The Primary Sampling facility has a single DCIS console, and the Radwaste Operations facility has a dual-headed DCIS console for monitoring and controlling operations. These both have similar layout arrangement and dimensions as the facilities in the MCR. Accordingly, my previous assessment comments for the DCIS console apply.

4.6.3.4 Access Routes

506 I have considered at a high level, the adequacy of access arrangements for typical work activities. I have not considered the adequacy of access routes relating to the safe and timely evacuation of personnel in an emergency, or the general accessibility of control rooms, panels and equipment in emergency situations. This is essentially the result of my

sampling and targeted approach to this assessment. In addition, mechanical engineering colleagues provide some consideration of general accessibility issues. (Ref. 178).

> ***AF-AP1000-HF-52*** *- The licensee shall consider the adequacy of access routes for the safe and timely evacuation of personnel in an emergency and the general accessibility of control rooms, panels and equipment in emergency situations.*

507 In the Local Panel and Maintainability Guidelines (Ref. 88) Westinghouse specify that *"Major access corridors should be a minimum of 7-feet (2,134-mm) wide; based on two people walking in one direction and a third person passing the other way"*, and that for *"maintenance access only, one-person corridors should be 26-inches (660-mm) wide, or 4- feet 7-inches (1,397-mm) wide for two persons walking or passing side-by-side"*. I consider that these provisions are adequate for the main access corridors. However, for maintenance access, I have noted that the minimum widths proposed by Woodson and Tillman (Ref. 162) are 30 inches (762 mm) and I consider that these figures should be used as the minimum. It is also necessary to note that these dimensions take no cognizance of any equipment that may need wider clearances still, such as trolleys or test equipment. The maintenance access dimensions should therefore be reviewed, and recognise the likely equipment (access) requirements. This can be undertaken by the Westinghouse COMIT process should their schedule permit. In addition, mechanical engineering colleagues advise that maintenance equipment can reasonably be broken down to facilitate access; and that they will take forward a prospective licensee's breakdown strategy as part of routine regulatory business.

> ***AF-AP1000-HF-53*** *- The licensee shall review maintenance access dimensions; recognising the likely equipment (access) requirements.*

508 Within the Local Panel and Maintainability Guidelines (Ref. 88) Westinghouse also specifies clearances around controls and control panels. I consider that these provide adequate space for effective monitoring and control.

4.6.3.5 Conclusions

509 I judge that the workstation designs offered are generally adequate, although I note minor issues that can be taken forward typically as V&V activities. The anthropometric data applied I do not consider fit for purpose and should be re-evaluated against recognised UK data.

4.6.4 Environment

510 These findings relate to item (3) from the methodology and scope presented in Section 2.2.9.1.

4.6.4.1 Lighting

<u>Normal Lighting</u>

511 I have assessed the lighting levels that are proposed in the Plant Lighting Specification (Ref. 161), which proposes the following levels:

- High levels of illumination are proposed in Medical Aid rooms (1000–2000 lux) and Laboratories (500–1000 lux).

- Between 200 and 500 lux is quoted for the Main Control Boards and Auxiliary Control Panels.
- An illumination level of between 500 and 1000 lux is quoted for the '*Operator's Station*' in Control Rooms.
- An average of 800 lux is normally maintained in the MCR and the RSR when off-site and/or on-site AC power sources are available.

512 I note that Westinghouse has stated that the lighting levels cited correspond to average/nominal levels, which take into account deterioration in light output and the impact of the room atmosphere and accumulating dirt. This will result in the installed illumination levels being higher than the levels specified by Westinghouse, to ensure that levels remain adequate despite ageing of the light sources and the build up of dirt on the luminaires.

513 In general, I consider that the proposed levels of illumination are appropriate for the tasks to be conducted. However, the stated maximum lighting levels for the MCR and RSR are far higher than necessary, although I note that a dimming function will be provided in accordance with mandatory guidance in the Plant Lighting Specification (Ref. 161), which states: *"The lighting in the control room should be dimmable between 250 and 500 lux"*. Often much lower levels are suggested for office work (e.g. in Kroemer and Grandjean (Ref. 132)) and these can also reduce problems from unwanted glare.

> ***AF-AP1000-HF-54*** *- The licensee shall provide additional justification that the lighting design of the MCR meets relevant standards and guidance.*

514 I am encouraged that Westinghouse states that the proposed luminaires have been selected based on consideration of factors such as glare, luminance ratios, contrast, shadows. However, there is no clearly described design process for how these factors are to be considered and managed, and I have not seen any evidence of the practical implementation of these criteria at this stage.

515 However, in summary I am confident that the lighting provisions lie within a range that will not degrade physical, perceptual or cognitive performance.

Emergency Lighting

516 In the December 2009 PCSR (Ref. 17) Westinghouse explain that the *"UPS [Uninterruptible Power Supply] system provides power to the emergency lighting in the main control room and at the remote shutdown workstation"* and elsewhere in the December 2009 PCSR (Ref. 17), they also indicate that "*The emergency lighting provides illumination in areas where emergency operations are performed upon loss of normal lighting. The panel lighting in the control room is designed to provide the minimum illumination required at the safety panels"*.

517 Detail regarding the proposed emergency lighting has been obtained from the Plant Lighting Specification (Ref. 161). Upon the loss of normal lighting, the Emergency Lighting System (ELS) provides lighting for the safety panels in the MCR and emergency area lighting in the MCR and RSR. For the first 72 hours power is provided by the Uninterruptible Power Supply (UPS) and thereafter by two ancillary Alternating Current (AC) diesel generators.

518 In the event of loss of both on-site and off-site AC power sources, the ELS provides eight hours of emergency lighting via self-contained battery operated lighting units. These will provide illumination of 20 lux along the access and egress routes assigned for fire fighting

and safe evacuation of buildings, and in other areas where recovery operations may be underway. I have noted that the provision of 20 lux is higher than the minimum levels quoted in BS 5266 (Ref. 163).

519 In general I judge that the proposed emergency lighting levels are adequate for the required tasks and that the emergency lighting provisions lie within a range that will not degrade physical, perceptual or cognitive performance, and will support required activities during a power outage. I have a minor issue regarding the effects of contrast where there is very low lighting in access routes and the lighting is not uniform.

4.6.4.2 Heating and Ventilation

Temperature

520 Ref. 133 describes the initial MCR temperature range as being between 19.4°C and 23.9°C. The range is close to the range specified in the HSI Guidelines (Ref. 105) of providing 20°C to 26°C in control rooms.

521 Ref. 131 states that the Radiologically Controlled Area Ventilation System (VAS) is to provide sufficient ventilation to maintain the ambient room temperatures within the following ranges:

- occupied areas, laboratories - 22.8-25.6°C;
- areas with electronic equipment - 18.3-29.4°C;
- areas of infrequent inspection - 10 – 40.6°C; and
- inaccessible areas - 10 – 54.4°C.

522 I consider the maximum temperature proposed for areas of infrequent inspection to be high at 40.6°C. Temperatures at this level will only be tolerable for short periods and could result in a negative impact on the quality of inspections due to the discomfort caused by these conditions.

523 The ponds area is traditionally one area where operators can be exposed to both high temperatures and high humidity. In the response to TQ-AP1000-423, Westinghouse stated that *"Localised cooling for the refuelling bridge crane operator is provided during refuelling operations by a dedicated packaged air conditioning unit furnished in accordance with spent fuel pool refuelling bridge crane equipment specification to control the wet bulb globe temperature below 26.7°C and a dry bulb temperature below 35.6°C for operator comfort."* These maximum permissible temperatures can be uncomfortable to work in, for any prolonged period and can lead to heat stress and exhaustion. Data in NUREG-0700 (Ref. 10) suggest that at temperatures around this level, with PPE assumed to be equivalent to 'double cottons', exposure to this level of heat should not exceed two hours. The response to TQ-AP1000-423 provided more detail on the proposed spent fuel pond environmental conditions. The maximum designed summer temperature is 35.5°C, with an estimated relative humidity of 45%. In winter, the designed minimum temperature is 10°C with a relative humidity of 40%. If prolonged work is required at the maximum temperature in the spent fuel pond area, then clear guidelines must be provided to ensure that appropriate work/rest cycles are adopted.

> ***AF-AP1000-HF-55*** *- The licensee shall develop appropriate controls as part of the work design for the spent fuel pond area, recognising the expected thermal environment in the area.*

524 In the MCR, I consider the specified temperature range is sufficient to ensure the thermal comfort of operators. However, for generally occupied areas and laboratories, I consider the entire temperature range of 22.8 to 25.6°C to be somewhat high. It is noted that the HSI Guidelines (Ref. 105) recommends a temperature of between 20 and 24°C in winter months. I do not expect this range will have a direct impact on human performance or safety.

Humidity

525 Only limited details about humidity have been identified. Humidity levels were defined for the radiation chemistry laboratories and security rooms, but no other humidity level details have been defined. The response to TQ-AP1000-423 provides assurance of acceptable humidity levels in the spent fuel pond area. However the response to TQ-AP1000-1082 provides no information on the range of relative humidity to be delivered in the MCR. I have only found limited details on humidity within the MCR and fuel handling areas. I consider that this is an omission in the HF justification and that this information should be provided. Where they have been stated, I consider the designed humidity levels to be acceptable. However, I consider the lack of any target levels for humidity and draught control in the MCR specification, to be an omission.

> ***AF-AP1000-HF-56*** *- The licensee shall provide information on and justification for the expected humidity in the MCR and fuel handling areas.*

526 Ref. 131 states that the Radiologically Controlled Area Ventilation System (VAS) will maintain the relative humidity of the radiation chemistry laboratories and security rooms between 35% and 50%. This is within the range of 30% to 60% recommended in Kroemer and Grandjean (Ref. 132) who consider that relative humidity of the air in the room should not fall below 30% in the winter and that a range of between 40% and 60% is considered comfortable in the summer.

Emergency Habitability

527 From detail obtained from the MCR Emergency Habitability Specification (Ref. 133), the initial temperature range expected in the MCR is between 19.4°C and 23.9°C.

528 In the event that the Nuclear Island Non-Radioactive Ventilation System (VBS) is unavailable for more than 72 hours, then ancillary fans maintain the MCR temperatures based on the temperature of the outdoor air supplied to the MCR.

529 It is stated that the bulk air temperature rise in the MCR pressure boundary shall not exceed 8.3°C during the first 72 hours following the loss of the Non-Radioactive Ventilation System (VBS). This gives a maximum expected temperature of 32.2°C given the initial expected MCR temperature range of 19.4°C and 23.9°C. Although the higher temperature will be uncomfortable, it is not expected to have any significant effect on human performance. The external temperature range assumed by Westinghouse to determine the estimated 8.3°C rise in MCR temperature was based upon weather conditions recorded in North Wales, which I consider appropriate.

530 Ref. 133 states that the Emergency Habitability System (VES) will limit the maximum temperature to 49°C in the DC equipment rooms and in the C&I rooms over a 72 hour period. If cooling is required beyond the 72 hours, the ancillary fans can be used to supply outside air to the C&I rooms and alternatively, the doors for any C&I room can be opened to establish natural circulation cooling.

531 It is stated in the MCR Emergency Habitability Specification (Ref. 133) that the VES shall maintain CO_2 concentration at less than 0.5% for up to 11 MCR occupants. I am aware

that feelings of drowsiness can occur from 1% CO_2 levels and hence the stated limit of 0.5% is considered acceptable. Furthermore, TQ–AP1000-423 states that the maximum CO_2 level in the MCR is 0.3% and I consider this to acceptable. Back-up protection to the permanently installed habitability systems consists of self-contained portable breathing equipment with air bottles that are stored in the MCR. These provide up to six additional hours supply of breathable air to be shared between the occupants. It is noted that an unlimited offsite replenishment capability is to be provided.

532 The MCR Emergency Habitability Specification states that the MCR relative humidity is expected to stay below 75% during the entire duration of the VES operation. Whilst an upper limit of 75% would be slightly uncomfortable, at 23.9°C this would not in my opinion detract from human performance.

533 In summary, I do not expect the humidity will have a negative impact on safety related actions.

534 I consider the design specification for temperature and humidity control during emergency conditions to be acceptable. I also find the projected CO_2 concentration levels to be acceptable in all conditions.

4.6.4.3 Noise and Acoustic Environment

535 Westinghouse's mandatory guidelines for noise levels are listed in Ref. 105 and state:

- The ambient noise level in the control room should not exceed 50dB(A), and noise peaks should not exceed 65dB(A).
- The reverberation [period] in the control room should not exceed 1 second.
- Persistent background noise level at local plant operating locations should not exceed 65dB(A).
- Where the intermittent environmental noise level can rise to 85dB(A) and above, suitable ear protection should be provided.

536 I commissioned an acoustic expert to assess the noise and acoustic environment in the MCR, using the Westinghouse document 'Evaluation of the Noise in the AP1000 Main Control Room' (Ref. 134). A detailed appraisal of the Westinghouse analysis is presented in Ref. 77.

537 In summary the general procedure focuses only on direct air-borne noise transmission and does not consider the possibility of structure-borne transmission of sound and flanking paths for air-born noise.

538 There is an over-reliance on theoretical acoustic formulae (in particular the mass law), which are normally recognised as being indicators, rather than actual, when transferred into the real world. Manufacturer data for some of the materials and doors would be more convincing than data derived from theoretical ideal calculations.

539 In addition to the lack of practical transmission data, there is no information on machine mounting or room acoustics (for example, acoustic treatment of the inside of the control room is likely to have a significant effect on speech intelligibility, irrespective of the noise level). There is also nothing stated about machinery inside the control room (Heating, Ventilation and Air Conditioning (HVAC), computer fans, etc) and how that might add to the noise level in the room.

540 There are some seemingly circular arguments used to justify noise levels outside the main control room (i.e. the maximum level allowed in a room is X, if we assume this, then the level outside must be less than Y, when we use Y to calculate the level in the room it is less than X).

541 Westinghouse presume that at noise levels lower than 50dB(A), the control room will be quiet enough to allow adequate speech communication appears to be based on a requirement in Ref. 1 to the report (Ref. 134). The level of 50dB(A) does not seem unreasonable, assuming that room reverberation is reasonably well controlled.

542 The objective of the Westinghouse report is to demonstrate that noise levels in the main control room are below the prescribed 50dB(A) limit. In my opinion the process used to estimate noise levels is weak, and may have overlooked important noise transmission paths. In many ways the important features of noise control are the way the structures are put together, e.g.:

- What happens when wall meets ceiling?
- Will the room spaces have vibration isolation between adjacent rooms?
- Do the rooms share common structural elements?

543 There is a mixture of using both substantially over-optimistic and substantially over-pessimistic assumptions about noise performances and noise environments. In part this stems from an over reliance on idealised acoustic formulae. I am therefore not able to be confident that the noise level will be as predicted by Westinghouse. Certainly elements such as the HVAC system are likely to be potential problem areas. But the calculations of noise levels from the main steam line dismiss this as a potential noise source, and I suspect that this may not be the case.

544 I consider that the route used to arrive at the conclusion has applied standard equations to airborne noise transmission with poor knowledge of the practical acoustics issues.

545 The assessment of speech intelligibility is often based on an ergonomics standard ISO 9921:2003 "Ergonomics – assessment of speech communication". I suspect that the requirement for 50dB as an upper limit for control rooms is somewhere based on this standard. However, 50dB(A) should be an upper limit. At 50dB(A) one may still suffer from intelligibility issues at 2m from someone talking normally (e.g. Annex H.1 of ISO 9921 shows an example of poor intelligibility rating for a background noise level of 51.7dB(A) for speakers 2m apart (Ref.167)).

546 I support the aimed reverberation time of 1 second, and on a practical level I consider that the passive cooling fins that are intended to be mounted in the ceiling offer potential to reduce reverberation by acting as baffles. However I have a minor issue relating to the noise transmissibility as the metal fins may make the room sounds quite bright, with high frequencies bouncing of the metal fins.

547 In summary I consider that there is further work required on the noise and acoustic design of the MCR, although I recognise that many of the solutions to problems in this can be developed as design progresses. I therefore consider this something to be taken forward by a prospective licensee organisation.

> ***AF-AP1000-HF-57*** *- The licensee shall reanalyse the noise and acoustic design of the MCR and provide additional HF justification.*

548 Outside of the MCR, levels of 45dB(A) are quoted for offices and up to 60dB(A) in the Diesel Control Room. The highest quoted level is at 85dB(A), which is estimated for the

Turbine Hall and Chillers room. I note that hearing protection will be required to meet UK legislation where levels are expected to exceed 85dB(A) and 80dB(A) if there will be prolonged exposure. However, as part of V&V the noise levels of such areas should be confirmed, particularly with regard to the audibility of general emergency alarms.

> ***AF-AP1000-HF-58*** *- The licensee shall ensure the audibility of general emergency alarms throughout the plant during V&V.*

4.6.5 Control/Display Interfaces and Alarms

549 These findings relate to item (4) from the methodology and scope presented in Section 2.2.9.1.

550 Westinghouse has developed three separate systems for the control and monitoring of AP1000. These systems are segregated from each other, such that they are functionally and spatially diverse, and offer independent ways to operate and monitor the most important process parameters. I consider the interfaces provided for each of these systems separately. The three systems are:

- DCIS;
- PMS; and
- DAS.

551 I have assessed the controls and instrumentation that are to be used locally on the plant. In addition, the operators will undertake some tasks on the LAN, often using proprietary software. However, as the LAN is not used for operational purposes, I have not undertaken any assessment of the LAN interfaces.

552 Westinghouse claims to have designed the instrumentation systems in the MCR such that in the event of a major system failing, there will be an alternative way to monitor the reactor and bring it to a safe shutdown. For example in the December 2009 PCSR, Westinghouse state *"To support the diverse manual actuations, sensor outputs are displayed in the main control room in a manner that is diverse from the protection system display functions"* (Ref. 17).

553 Westinghouse also claims to have taken a consistent approach to the design of the human interfaces. For instance, for soft control interfaces, the Instrumentation and Control[7] (I&C) Specification (Ref. 135), specifies that: *"Operator workstation soft control interfaces shall be unique and used consistently"*. I assume this means that the interfaces are specifically designed for each display or pop-up such that they can be recognised for that particular application, but that common interface elements are used consistently.

554 Similarly the HSI Guidelines (Ref. 105) state that *"The application and design of soft controls should be applied consistently across all HSI resources"*. Elsewhere in the HSI Guidelines there a mandatory requirement that *"HSI control and display design and operation philosophies should be applied consistently throughout the plant"*.

[7] 'Instrumentation and Control' is US equivalent of 'Control and Instrumentation'. The terms can be used interchangeably. Used in place of UK term 'Control and Instrumentation' in this document when specifically referring to WEC documentation or practice.

Between-System Display Design Consistency

555 In terms of ensuring consistency of the coding conventions, control movement conventions, control/display relationships, icon usage and terminology on the three main C&I systems within the MCR, I consider that the development of the HSI guidelines for the software display components (Ref. 105) provides a basis to ensure that all the DCIS and PMS display pages conform to a similar design. However, I have noted three discrepancies between the DCIS and the PMS displays that I feel merit comment.

556 The first discrepancy relates to the way that colour coding had been applied. This involved the convention whereby 'Green' signified a lower energy state (i.e. a 'closed' or 'off' condition), whilst 'Red' signified the opposite. Within the DCIS displays this appeared to be interpreted as meaning that 'Green' was the 'de-energised' condition. Hence, within the DCIS displays, electrical breakers were coloured green when they were open, as there was no electrical flow (as defined in Table 22.1-1 of Ref. 105). In contrast, on the PMS the opposite was true and 'Green' was used when breakers were closed. This could promote human unreliability.

557 The second discrepancy was that the design of controller interfaces for PMS that is presented in Ref. 136 differs in both the relative position of the vertical bar displays and the terminology used, from the equivalent interfaces proposed in the HSI specification (Section 4.3 of Ref. 136). I note that this may result in an increase in human error potential.

558 Most of the PMS displays are structured lists of parameter values or status indications and I did not have similar DCIS display pages with which to compare them. However, there are five displays that contain some graphic representations of the particular processes; hence I was able to compare the graphic display for the IRWST display page for PMS with one of the IRWST pages for the DCIS. It appeared to me that similar information was being presented differently. I did not have sufficient information to judge the impact of this, but if more detailed examination of all the IRWST display pages corroborated this, consideration should be given to redesigning the layout of the PMS page to more closely match that of the DCIS.

559 However apart from these minor discrepancies, I judge that the displays and controls on the different interface systems were reasonably consistent between each other, such that human errors would not be unnecessarily induced (subject to the discrepancies noted previously).

560 In terms of measures taken to prevent accidental operation of controls within the MCR, I consider that the design and positioning of the controls should prevent accidental operation of the controls. The requirement to operate controls at both the PDSP and the SDSP simultaneously should effectively minimise the risk of precipitate operation of controls which have onerous consequences.

Distributed Control and Information System

561 A detailed overview of the design of the DCIS, including screen formats is presented in Ref. 77.

562 I consider that the choice of a light grey background and the avoidance of saturated colours results in graphics and text are highly legible, and generally, the colour and brightness contrasts are good. The decision not to colour-code the contents or functions of different flowlines is interesting, but for the graphics that I have examined, it works well. Similarly, the two line thicknesses work well together and can be readily differentiated.

The Windows bars at the top of the page use icons and interface concepts with which most users will be well acquainted.

563 The Navigation Top-Level page is identified as being at Level 1, although there is another Level 1 page. The next level down at Level 2 is termed an Overview page; although there is another Level 2 page that provides a detailed graphic. I note two minor observations: the word 'Overview' is normally used in hierarchical systems to describe the Top Level page and hence is potentially confusing. Secondly, the downward navigation to another page of greater detail that is designated to be at the same level is conceptually incoherent. This structure also means that the detailed component-level displays are at Level 5 in the hierarchy, rather than the nominal Level 3 that is described. NUREG 0700 (Ref. 10) and the HSI Guidelines (Ref. 105) both recommend that a maximum of three levels in a menu hierarchy are appropriate, but elsewhere (Ref. 105) it is stated that a five level hierarchy is acceptable. I agree with Westinghouse that a five level hierarchy is acceptable; provided that there are sufficient task-based cross links to limit the need to navigate vertically through the hierarchy and particularly to avoid the use of all five steps contiguously.

564 For navigation to the System Oriented Displays, the provision of alternative navigation facilities between different display pages has been well implemented and should enable the operators to move rapidly between displays as required during predictable scenarios. In particular, the comprehensive facilities that are provided should enable operators to respond quickly to unexpected situations. Therefore, I consider from viewing a limited sample of the System Oriented Displays, that this supports Westinghouse's claim "Accessing a display or window that is directly related to the current display should be accomplished using a single action" (Ref. 105). However, the overall menu structure is complex.

565 I consider that the display pages that were accessed from the Overviews were generally clear; however I note that there were very few references to other systems.

566 A fundamental requirement in the use of colour coding is that colour should always be redundantly applied with another form of coding. Westinghouse has attempted to do this in the way that they have coded the physical status of plant items, by using broken lines as well as the plant item status within the symbols. However, I do not consider that this gives a particularly strong visual cue, and should be reconsidered. I also have a general minor issue relating to descriptions used throughout Westinghouse's documentation for red and green colour-coding. I would prefer to see these two colours described in terms of their energetic state, rather than to the specific conditions of particular components. Thus, green would represent a de-energised state, whilst red would represent an energised state.

567 I recognised the potential impact on human reliability that could result from differences in population stereotypes against the generic AP1000 interface design, which recognises US population stereotypes. In response Westinghouse commissioned some research into UK and US population stereotypes and provided an impact assessment against the generic interface designs (Ref. 137). I was not able to assess this document within GDA Step 4 timescales; however I will require a potential licensee organisation to consider this work against the generic interface designs, and for it to feed into the V&V programme.

> ***AF-AP1000-HF-29*** *- The licensee shall review the Westinghouse work on UK national population stereotypes; provide an impact assessment on the generic design of HMIs and justify how the UK AP1000 final interface designs comply with national population stereotypes. This should also form part of the V&V programme.*

568 I consider that the use of a sans serif font that is specifically designed for screen displays is a good choice. I do not have enough information about the screen size of the text to be able to comment on its legibility. I also note that a labelling hierarchy is being used, but feel that this should be more pronounced. My calculations indicate that the height of the text in most of the superordinate label levels only increases by 10 to 20%, when the accepted practice to distinguish between text by size is at least a 25% difference in character height at each step in the labelling hierarchy. This negates the value of the perceptual cues in the labelling hierarchy. In addition, Westinghouse has specified a hierarchy of eight levels when most recommendations, including NUREG 0700 (Ref. 10) would confine a scheme to three or four levels. This should be reconsidered.

> ***AF-AP1000-HF-59*** *- The licensee shall reconfigure the labelling hierarchy on the DCIS screen displays proposed by Westinghouse against recognised good practice in this area.*

569 I note that the DCIS interfaces rely heavily on abbreviations. I do not consider the predominant use of abstract and often meaningless item identification codes to identify most items on the DCIS displays complies with good practice, particularly as these often do not correspond to meaningful acronyms. The system descriptors are always presented in upper case characters and that for the vast majority of items on a given mimic there are exactly three characters. Therefore, the operators must rely upon reading the numerical string to differentiate items. This places a considerable memory burden on operators for correct recall. This is a retrogressive step. Sizewell 'B' has functional descriptors for the majority of displayed plant items to avoid incorrect functional interpretation or recall. This was applied as a result of operational experience and incidents where confusions had occurred due to reliance on plant item numbering rather than functional names, which led to human errors.

570 I consider that the symbol set applied to represent the different types of component is clear and that this is consistent with the expectations of workers in the UK NPP industry.

571 I consider that Westinghouse has presented process data and alarm set points clearly, and that in particular, the colour-coding of parameters that are in alarm is very effective.

572 The pop-ups appear to me to be generally clear and well designed. However, I note that the terminology that is adopted to label the vertical scales on flow controller pop-ups is unclear and inappropriate. As these are particularly important interfaces, I feel that this labelling should be reconsidered.

> ***AF-AP1000-HF-60*** *- The licensee shall reconsider and justify the terminology that is adopted to label the vertical scales on flow controller pop-ups on the DCIS.*

573 In making an overall assessment of the acceptability of the DCIS interfaces I have had to rely upon the evidence presented by guidelines and design requirements rather than upon evidence of completed display designs. However, I have found such guidelines and requirements to be generally very comprehensive. These documents include a large number of specific design requirements and specifications, and virtually all of the individual items are underpinned by good HF advice. I agree with the vast majority of these although I consider that a few are a little dated or trivial, particularly for computer-based displays.

574 I consider that the Specification for the Display Elements (Ref. 138) adequately fulfils my requirement from the HMI TAG T/AST/059 (Ref. 7) that *"A HMI style guide or similar document, based on agreed HMI requirements and specifications, should be developed*

by the dutyholder to demonstrate the philosophy underlying the design". However, many of the guidelines are not mandatory, and in the absence of a complete set of DCIS formats, I have not been able to fully examine the effectiveness with which they have been implemented.

575 In summary the DCIS design generally conforms to accepted good practice. I have minor issues with particular aspects of the design; and these should be explored during subsequent V&V activity (Assessment Findings AF-AP1000-HF-27, AF-AP1000-HF-52 and AF-AP1000-HF-53 refer).

Wall Panel Information System (WPIS)

576 Westinghouse claim that the WPIS provides a semi-permanent display for important plant information. For example, in the UK HF Safety Case (Ref. 35) Westinghouse state *"The inclusion of the large screens (WPIS displays), providing immediate information on alarms to the operator is readily visible from all areas of the MCA* [Main Control Area]. *The WPIS also provides information on the overall plant status, key plant information, with important or critical information being displayed at fixed locations on the WPIS at all times. This is particularly advantageous in circumstances of relatively high workload."* In addition Westinghouse claims that the WPIS *"Provides an 'at a glance' overview of plant status"*.

577 A description of the WPIS is provided in Ref. 77.

578 Display legibility is influenced by the viewing angle. I consider that the most demanding viewing angle is from the SRO console. I estimate from the MCR plan (Ref. 125) that the widest viewing angle to the edge of the main array of the current (65") displays at the back wall is approximately 35º. According to the hardware specifications (Ref. 139) the outside WPIS screens are angled inwards by 30º) and I do not consider that these viewing angles will seriously degrade legibility due to foreshortening.

579 My subjective impressions from the simulator visit are that legibility should not be an issue, but this should be confirmed by calculations based upon the actual character sizes. As these display pages will be based upon the DCIS displays, I have the same concerns about the absence of functional labelling to those highlighted earlier for the DCIS. I consider that the display of process parameters and associated units will be clear. I also consider that the data which are to be displayed on the main set of WPIS displays are appropriate for the process overview and alarm overview roles for which these displays are intended. The 'heartbeat display' meets my criterion for indicating the health of the WPIS displays.

580 My judgements about the software interface are similar to those made for the rest of the DCIS. Westinghouse's decision to dedicate most of the WPIS to particular displays means that there are few navigation concerns. However, I do consider that it would be useful to provide users with feedback relating to the display pages on particular screens that have automatically changed after a reactor trip; by using a non-intrusive form of coding, such as the use of a different background colour or border.

Protection and Safety Monitoring System (PMS)

581 The PMS has been designed to reduce the risk of inadvertent operation of some controls, where there have been judged by Westinghouse to have potentially 'onerous consequences', which they have defined as *"… causing a breach of the reactor coolant system (RCS) pressure boundary or a need to shutdown the plant to cold conditions to effect repairs"* (Ref. 140). This supports Westinghouse's claim in the Design DCD for the European AP1000 (Ref. 64) that *"Incorporating human factors engineering in the design and testing of the main control room reduces the likelihood of the operators either*

inadvertently causing a fault sequence, or performing the wrong actions during a fault sequence".

582 A description of the PMS is provided in Ref. 77.

583 I consider that the switch sections of the PDSP are well arranged and clearly labelled. Those switches that are also shown on the SDSP are identified on both the PDSP and the SDSP by using a light blue background, which gives a very clear cue that these controls are twinned with similar controls on the PDSP. The label legends are consistent between the two panels. However, the spatial arrangement of the switches labelled 'IRWST INJECTION' and 'IRWST RECIRCULATION' are transposed between the PDSP and the SDSP. This could lead to selection errors. Therefore, one of these panels this should be modified to reflect the task order in which they are used. Otherwise, I consider that the overall design of these two panels has been well implemented and will provide effective protection against both inadvertent operation and the consequences of single switch failure.

> ***AF-AP1000-HF-61*** *- The licensee shall redesign the PDSP and SDSP to remove the transposing of 'IRWST INJECTION' and 'IRWST RECIRCULATION' controls or justify the existing design.*

584 I consider that the PMS display pages are usable, but I also found it difficult to develop a mental model of how the constituent pages related to each other. Therefore, I was left with the impression that there could be a potential that when an item such as an interlock was overridden from its normal condition, this may only be shown on a bottom-level display. I also considered that several of the pages were relatively crowded with information.

585 I compared one of the PMS formats with the equivalent DCIS format, and on this particular display I found it difficult to relate the information from the two sources. I consider that this issue requires further investigation as it could increase the error potential if the PMS was required post fault.

> ***AF-AP1000-HF-62*** *- The licensee shall ensure the consistency of information content and presentation between equivalent PMS and DCIS formats.*

Diverse Actuation System (DAS)

586 I have no issues with the interfaces on the DAS panel.

Remote Shutdown Room Controls and Displays

587 A description of the remote shutdown room is provided in Ref. 77.

588 The DCIS interfaces at this workstation are identical to those provided at an RO's workstation; hence no further comment is offered here.

589 I have no issues with the individual controls on the RSWP. However, I note that the spatial arrangement of the RSWP controls is different to the spatial arrangements of the corresponding controls on the PDSP and the SDSP in the MCR.

590 On the PDSP all of the controls are duplicated to ensure that any of the Engineered Safety Features (ESFs) can still be manually actuated in the event of a single switch failure. In addition, to provide protection against inadvertent operation of controls that could have potentially onerous consequences, the controls are repeated on the SDSP and they must be operated coincidently to actuate the related functions. This situation is not

replicated on the RSWP; the switches provided here are manual backups to automatically generated PMS trips. On the RSWP, controls for ESFs with non-onerous consequences are not duplicated; the intention being that any required second action is performed local-to-plant. Controls for actuating functions with onerous consequences are duplicated on the RSWP. On this panel, redundant controls are located together unlike within the MCR on the PDSP and SDSP; although I note that this separation is to minimise the effect of fire within the control panels. I also consider that it is unnecessary to locate some of the controls below each other on the RSWP. This arrangement breaks the perceptual link with the PDSP and the SDSP, which could impact the human error potential. Therefore, I consider that current layout of the RSWP controls should be reconsidered.

> ***AF-AP1000-HF-63*** *- The licensee shall reconfigure the* Westinghouse *proposed layout of the RSWP controls in relation to the equivalent layout in the MCR on the PDSP and SDSP.*

Local to Plant Controls and Displays

591 Westinghouse's approach to local-to-plant tasks has been to attempt to ensure that plant actions that can impact safety are undertaken from the MCR rather than locally. Therefore, most of the human actions that were assessed in the PRA were undertaken from the MCR, as per Westinghouse's claim in the December 2009 PCSR (Ref. 17) that *"Almost all operator actions credited in this PRA are performed in the control room; there are very few local actions outside the control room"*.

592 Similarly, Westinghouse claim elsewhere in the December 2009 (Ref. 17) PCSR that *"All the isolation valves are actuated by the containment isolation system; in addition, they can all be actuated manually from the main control room"*.

593 Where plant that is not monitored in the MCR has to be monitored locally, Westinghouse aim to ensure that any associated alarms are relayed to the MCR. In this regard I assume that this will involve a group alarm, which then requires a local-to-plant operator to investigate and identify the specific alarm. I did not identify any generic or specific claims, but on several occasions within the December 2009 PCSR (Ref. 17)there were statements about requirements for local-to-plant monitoring at specific locations.

594 I consider the design guidance for local-to-plant controls and displays reasonably comprehensive, and that the controls and displays for which guidance has been provided are the types of controls that will be provided on plant. I also consider that the guidelines are generally appropriate and in conformance with accepted HF practice.

595 The list of control/display relationships is presented as Table 9.1-1 of the guidelines and I consider that this complies with accepted population stereotypes for UK workers.

596 I note recommendation 10.1.8 that *"illuminating pushbuttons should not be used"*, as I consider that these are particularly appropriate for many local-to-plant actions. However I do concede that separate displays avoid the indication being obscured by the actuating digit.

597 Regarding the detailed guidance on gloveboxes, valve controls and Closed Circuit Television (CCTV) systems, I consider that this generally complies with accepted HF practice. However I consider that specific guidance should be provided about different types of manual valve controls, such as wheels or levers. I note that such guidance is provided by Westinghouse in design specification documents for different valve and component types. However, such information could beneficially be added to the general guidance offered as this affords greater opportunity for consistency. In particular, an

indication should be provided of the maximum permissible operating forces that should be applied, and the separations required between particular valve controls. This was also highlighted by a finding in a HF assessment of the local panels (Ref. 86), that there was insufficient clearance between several valve control wheels.

> ***AF-AP1000-HF-64*** *- The licensee shall ensure that the use of manually operated valve controls does not exceed the maximum permissible operating forces that should be used, and that the separations between valve controls do not hinder their use.*

598 I have not been able to obtain detailed design proposals for any of the local-to-plant controls and displays, therefore I have had to rely heavily upon design specifications, which may, or may not, be achieved in the actual plant. I conclude that the interfaces that are proposed appear to comply with accepted HF guidance and that the directions of control movements comply with UK expectations and population stereotypes.

4.6.5.1 Alarms

599 I note that the alarm system design that I assessed was not finalised and has since progressed, and that the design I assessed was subject to HFE trials (HFE Phase 3 Test; Ref. 143 refers), which produced significant comments. I acknowledge that Westinghouse's design process will address the Phase 3 test comments, and that this will result in a changed alarm system design to the one that I assessed. I considered the design available to me at the time in terms of a generic human reliability performance shaping factor to underpin the HRA. Therefore it is appropriate that a prospective licensee analyses the resultant generic alarm system design and justifies the alarm philosophy and detailed design in a UK context.

> ***AF-AP1000-HF-65*** *– The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.*

600 The Westinghouse claims made upon the Alarm presentation System (APS) are for the delivery of particular alarms to operators within the MCR. There are no claims upon specific design aspects of the alarm system, but rather upon specific alarms or upon the reliability of the operators in the processing of alarms. Within the December 2009 PCSR (Ref. 17) there are at least 30 specific claims made on alarms. For brevity I have included these in Ref. 77.

<u>Alarm Philosophy</u>

601 The APS Functional Requirements (Ref. 141) specify that any alarm must require operator action. It also sets out the requirement for alarm prioritisation and provides a general definition of each priority level. In addition, they specify that no greater than 5% of all alarms should have the highest priority (Priority 1). A cross reference is provided to a further document which specifies a basis for calculating operator response times as a determinant for setting appropriate alarm thresholds. All of these requirements are consistent with the guidance provided by the EEMUA (Ref. 142), which is a recognised good practice in this area.

602 However, there is no design process for identifying what should be included (such as that recommended by the EEMUA guidance) within the alarm population, or an indication of the likely number of alarms that will be present during key faults. It is important to identify

specific alarms that are critical, significant, or related to nuclear safety. I would expect to see a positive linkage between risk assessment processes such as FMEAs or Hazard and Operability studies (HAZOPs) and the alarm definition process, but I have found no evidence of such.

> ***AF-AP1000-HF-66*** *- The licensee shall justify that the specification of the alarm system provides an alarm for all safety related parameters / systems that require an operator response.*

603 There are seven types of alarm suppression or logical reduction described in the APS Functional Requirements (Ref. 141), each of which is conducive to logical alarm reduction when used appropriately.

604 In addition there may be an issue with the grouping of alarms. Grouping that is not supported by sufficient information can lead to an assumption of the recurrence of a pre-existing fault or a commonly occurring failure, when a new fault actually exists. This may also reflect a failure to correctly implement a fundamental change in the operators' approach to alarm system use, which is required in a rigorously implemented logically reduced alarm system

605 Fundamentally, an alarm system cannot be used for fault diagnosis as it merely captures the transgression of a series of thresholds that are pre-programmed into the system. The dynamic appreciation of a NPP requires the interrogation of key dynamic parameters and their transient performance, except in straightforward cases where an isolated equipment fault exists.

606 I consider that the design of the alarm system may be used by Westinghouse to serve as a substitute for a diagnostic engine. Westinghouse provide an example of the use of the cut-out function that is applied when a low flow alarm is suppressed given that a pump is in a stopped state. However, this form of logical signal conditioning is not always appropriate. If an operator manually stops a pump, the subsequent occurrence of a low flow alarm would be unnecessary. However, if the pump fails to a stopped state (e.g. due to over current protection), then a cut-out function could also disable the low flow alarm. In fact, the low flow alarm is a functional indication of pump failure and therefore must not be suppressed in that circumstance.

607 Of the two alarms (pump state and flow), the low flow alarm is more powerful, because it is sensitive to all deviations of the pump from functional success. For example, a low flow alarm will indicate impellor faults and upstream blockages as well as any faults arising in the pump prime mover.

608 If the pump is part of a duty standby scheme it would be appropriate for the low flow alarm to be suppressed, conditioned by the standby demand. (Of course, the duty standby scheme may well require complementary logic to ensure reliable alarm conditioning commensurate with the overall alarm system reliability).

609 Examining this particular instance further, it is more appropriate to remove the pump stopped alarm completely and rely on the low flow alarm as sufficient to draw the operator's attention to that pump failing. Therefore, in this and many other cases it is possible to avoid the use of the cut-out function entirely; provided that designers accept that alarms are a cue to a requirement to make a diagnosis, rather than an attempt to engineer a causal indicator system. That is, alarms are the prompt for an operator to interrogate the process state. This instance has been discussed at some length, as it points to the fundamental fact that many candidate alarms can be removed entirely from

the population, provided that it is accepted that alarms are not a diagnostic engine, but a cue to the need to make a diagnosis.

610 The APS consequence function directly suggests that the alarm system is intended to be used as a substitute for an operator diagnostic task. However, while such a feature will appropriately identify failures with systemic effects such as loss of bus faults and loss of an instrument air manifold pressure, the application of the consequence logic could suppress alarms that are actually of greater significance to nuclear safety, albeit not the root cause of the event. Therefore, I have concerns about the implementation of this function as defined in the Westinghouse documentation.

611 I note that the grouping function which constitutes part of the interface delivery is a de facto logical alarm reduction mechanism. However, this does not appear to have been recognised as such within the design process. This may also in part explain why users had concerns about insufficient information, as reflected in the Phase 3 Test Report (Ref. 143).

612 I conclude that the alarm population definition and reduction process for the APS is not clearly defined and that the resulting alarm interface is operationally deficient in the information presented. I further conclude that this may be partly due to an attempt to design the alarm system for diagnosis rather than as a system to generate cues indicating that diagnosis is required. This should be investigated further as part of the V&V process

> ***AF-AP1000-HF-65*** *- The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.*

Alarm Interface Design

Alarm Ownership

613 The routine users of the alarm system in the MCR are two *RO*s and a SRO. One of the *RO*s will typically be responsible for the primary reactor systems, whilst the other will be responsible for the balance of plant. Both of these *RO*s can perform alarm handling and monitoring activities from their respective workstations. Within the documentation supplied by Westinghouse I could not determine whether it is possible for two *RO*s to handle each other's alarms. However, I note that there are only two audible signals for process alarms within the MCR which are related to levels of priority, not ownership.

614 Some alarms are of separate functional use to primary side operations and secondary side operations, and therefore need to be handled at different times. There could potentially be unique, or multiple ownership, or rules of ownership for particular alarms. However, I have been unable to find any rules on alarm ownership between the two ROs. These should be clearly defined by a prospective licensee.

> ***AF-AP1000-HF-67*** *- The licensee shall clearly define the rules on alarm ownership, recognising the defined MCR staffing structure.*

615 The issue of alarm ownership and multiple ownership has not been addressed by the current APS design. In human performance terms, this can result in task disruption and the potential for increased human error.

Audible Annunciation

616 At the time of my assessment the alarm sounds were not finalised, and I acknowledge that Westinghouse have now progressed the design. My assessment considered the

sounds that were in place during Engineering Test 3. At this time there were three alarm sounds.

- High priority alarm (Priority 1 alarm). This alarm was a deep low buzzing, foghorn style sound with short pauses between long continuous sounds.
- Regular priority alarm (Priority 2 and 3 alarms and operator-defined alarms). This alarm sound appears to be a higher pitched trilling or warbling sound that is pulsed (similar to a telephone).
- Return to Normal chime (one-shot) when alarms clear.

617 The high priority alarm occupies greater time than the regular priority. However, I consider that the lower pitch and harmonic structure of this alarm will be naturally be perceived as sounding less important than the regular priority alarm. Therefore, this is a potential source of confusion for priority interpretation.

618 I note that a separate audible tone is not used for each level of priority. It is particularly important that this should be incorporated as operators have the option to set up their own alarms, which should be distinguished from those that are preconfigured within the process. In effect, this is to be used as a 'kitchen timer' which annunciates the arrival of an expected event as opposed to the unexpected events annunciated by priority 1, 2 and 3 alarms. I note that the functional guidance has been constrained by the assertion given within the EEMUA guidance (Ref. 142) that there should only be three audible tones. I consider that this constraint is overly restrictive and only relevant when the audible alarms comprise single frequencies or have a simple harmonic structure. It is entirely credible that alarm systems can be constructed to address the issue of ownership and priority to give a larger total population of alarm sounds. For example, the aviation sector has demonstrated alarm schemes with over 10 unique alarm sounds and modest learning. I therefore consider that the issue of alarm sounds be reconsidered; particularly with regard to ownership and priority notification.

> ***AF-AP1000-HF-66*** *- The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.*
>
> ***AF-AP1000-HF-67*** *- The licensee shall clearly define the rules on alarm ownership, recognising the defined MCR staffing structure.*

619 The 'return to normal' chime is not considered necessary and is an unnecessary distraction, as it draws the attention of the operator to the alarms interface when there is no action necessary. I note that the use of such a chime is common in US NPP with the intent that it provides the operators with feedback information to indicate that their actions have been successful; however I consider that this should be removed.

> ***AF-AP1000-HF-68*** *- The licensee shall remove the 'return to normal' chime within the APS, as it draws the attention of the operator to the alarms interface when there is no action necessary.*

620 I note Westinghouse's intention to suppress audible alarm signals of lower priority when higher priority alarms exist. This is appropriate, but should only been applied within the boundaries of alarm ownership.

621 It would also be useful for Westinghouse to demonstrate whether individual alarm sounds can be reliably heard if different priority alarms are activated simultaneously. In addition,

the alarms should be able to be heard and discriminated reliably in a realistic acoustic environment that contains other audible signals and noise such as printers, telephone ringers, HVAC fans and conversation. This should be incorporated into the V&V programme.

> ***AF-AP1000-HF-66*** *- The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.*

622 Alarm sounds are silenced by acknowledging the alarms. As new alarms activate, the audible signal is re-triggered. It is possible for operators to manually select an extended silence of all audible alarm signals for 5, 10 or 15 minutes. I assume that this facility is provided with the intent to avoid distraction after operators have recognised that there is an immediate problem that will result in many alarms. This is inconsistent with typical UK practice and I am concerned t2at the cancellation of the audible signal, even for short periods may hinder the operators' ability to recognise further unexpected events perhaps not associated with the initial fault.

623 This issue warrants further investigation, and should be subject to experimental trial to justify that this global silencing of alarms does not adversely affect human reliability.

> ***AF-AP1000-HF-69*** *- The licensee shall undertake experiments to demonstrate that the global silencing of all alarms will not significantly affect human reliability. This warrants specific attention and a more concentrated focus above that of a V&V programme.*

624 I note that the functional requirement is that audible alarms should be 15dB above background noise. An increase of 3dB is perceived as twice as loud, and when an audible alarm scheme is well designed, will readily penetrate any typical MCR noise at this level. Therefore, I consider that if the alarms are 15dB louder than the background level, this is likely to disrupt trains of thought, telephone conversations and technical discussions. I consider the audible alarm level of 15dB to be excessive and audibility should be ensured by distributed alarm system loudspeakers set to a lower level; consistent with audibility and non-interference with other tasks. This level should be set at commissioning.

> ***AF-AP1000-HF-70*** *- The licensee shall reassess and justify the audible alarm levels proposed by Westinghouse. I consider the current proposals to be excessive and likely to cause disruption. This should be specifically investigated during V&V and set prior to commissioning.*

Alarm Colours

625 There are four alarm priorities, highlighted by the background colour of the alarm tile being displayed in one of the following colours:

- Red (Priority 1);
- Orange (Priority 2);
- Yellow (Priority 3); and
- Light blue (User defined).

626 A user-defined alarm could be acceptable provided that it is not used as a substitute for inadequately defined safety critical, significant or related alarms. A user reminder or action prompt (i.e. a *'kitchen timer'*) is a valuable facility in the context of process control. However, it should not be used as a panacea for inadequate alarm system design.

627 All alarms are shape coded with a triangle. In addition, it is noted that the yellow appears brighter than orange and the cyan is brighter than both. Furthermore, European safety sign legislation results in the yellow colour having a strong association with hazards and warnings. I consider that this could, together with its brightness, be misinterpreted as a higher priority than the orange alarm. As an absolute minimum, I consider it necessary to use redundant shape-coding in conformity with standard HF requirements to assist in emphasising alarm priorities. In addition, colour intensity should be adjusted to ensure that more important alarms have increased brightness, and hence an increased attraction capability over less important alarms. Orange can also be confused with both red and yellow. Therefore, it is important that the clarity of the colours, and the ability to distinguish between them on the workstation screens and WPIS, is assessed in the ambient lighting conditions.

> ***AF-AP1000-HF-71*** *- The licensee shall specifically include the clarity of colours and the ability to distinguish between them on workstation screens in the ambient lighting conditions as part of the V&V programme.*

Alarm Presentation on the Wall Panel Information System

628 Alarm information is presented permanently on two dedicated display screens of the WPIS. The alarms for the Primary/Nuclear Island system are shown on the left panel, and the Secondary/Balance of Plant system is displayed on the right panel. Within each panel, alarms are presented using a continuously visible tile-based fixed layout. At the top of each dedicated alarm page on the WPIS there are four rows of alarm tiles for the 'System Group' alarms. Each of these tiles contains a three letter system designator. Below these are six rows of larger tiles for functional alarms, which are termed 'Important Group' alarms (e.g. Reactor trip, Pressurizer).

629 It appears that there are 53 three-letter system designator codes that are applied on the primary system group alarm tiles, and 37 similar codes that are used on the secondary system group alarm tiles. In addition, there are several other codes on the Important Group Alarm tiles. Many of these contain abstract codes rather than meaningful acronyms and abbreviations. This could result in misunderstanding by the operators. It should be demonstrated that the codes and abbreviations are readily understood, and that sufficient meaning can be obtained from the alarm tile information for them to be of practical use.

> ***AF-AP1000-HF-72*** *- The licensee shall demonstrate that the codes and abbreviations proposed for the primary and secondary system group alarm tiles are readily understood and are of practical use to the operators.*

630 The background of an unacknowledged alarm will blink with the priority alarm colour (the text does not blink), and I note that the tile colour blinks on/off approximately once a second, which meets the minimum requirements defined in Ref. 141. I further note that the flash rates are the same for different priorities and hence the higher priority alarms are not visually more 'attention attracting' as would be expected in accordance with Ref. 141. I acknowledge that redundant forms of coding are applied, and Westinghouse consider

these to be sufficient (colour and noise). However, consideration should be given to the application of differing flash rates to support this coding system.

> ***AF-AP1000-HF-73*** *- The licensee shall consider the benefit of differing flash rates for different alarm priorities, to supplement the current coding of alarm prioritisation.*

631 The black text changes from normal to bold on the flashing tiles when an alarm is present. The alarm colour will then become steady when the alarm is acknowledged. I consider that the text remains legible when the background of the tile is flashing. The flashing is synchronised on the screens.

632 A Status Bar provides an alarm summary. This includes information on how many alarms are new, acknowledged etc., and a spinning icon that acts as a *"heartbeat"* to show that the system is receiving live data. These features do not require much physical space on the screen and I consider them to be useful additional information.

Alarm Presentation on the Distributed Control and Information System

633 The alarm system information can be presented on any one of the screens at each dual-headed DCIS workstation used by an *RO*, or the SRO. When presented on the workstation, client alarm tiles occupy the top horizontal section of the screen, and a user-selected or default alarm list on the bottom half.

634 However, I note that for the Sizewell 'B' workstations, user trials established that it was necessary to have a screen dedicated to alarms; resulting in a total of five screens for an *RO* workstation at Sizewell B.

635 I consider that there should be a clear demonstration that four screens will be sufficient to support concurrent process and alarm systems monitoring, without undue display system reconfigurations that disrupt interactions within the plant. This demonstration must also consider that in an emergency one of the available screens will be used to present the EOPs or AOPs.

636 Transgressed alarm thresholds are also usefully embedded in process mimics.

637 When all audible alarms have been silenced, the operator can still potentially identify a new alarm from the flashing of alarm tiles. However, the only reminder that the alarm sounds have been silenced is a greyed out icon with slanted text on the toolbar, which is difficult to differentiate. I do not consider alarm silencing, in this regard, appropriate and it should not be implemented for the UK design.

638 I consider that the fundamental effects on human reliability of silencing all audible alarms, and the indications to the operator of this action have not been carefully considered. Additional safety justification should be provided in this regard.

> ***AF-AP1000-HF-69*** *- The licensee shall undertake experiments to demonstrate that the global silencing of all alarms will not significantly affect human reliability. This warrants specific attention and a more concentrated focus above that of a V&V programme.*

639 I note that there are options for the operator to personally configure large aspects of alarm presentation on the DCIS, including font sizes and alarm list structuring for example. I consider it preferable for Westinghouse to define an optimum design based on recognised good HF practice, and prescribe its implementation; this avoids personal configuration employing sub optimal ergonomics; which may compromise human reliability, for example by inducing misreading errors. Consideration should also be given to SAP ESS.15 in this regard (*"No means should be provided or be readily available, by which the configuration*

of a safety system, its operational logic or the associated data (trip levels etc) may be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.").

640 I note various minor points of ergonomics relating to the design of the alarm list columns; however I consider that they contain all the information that will be logged. In my judgement there is more than is necessary for operational purposes and superfluous information is contained within fields (e.g. some date time stamping and insignificant digits). This all detracts from rapid comprehension.

641 I also note that the terminology in alarm lists is not the most meaningful, either due to incompatibility with UK practice, or due to unnecessary or the untested use of abbreviations. For example, 'Pri' means priority which could easily be vulnerable to reader block and be read as 'Primary'. Also, it is unclear what 'CO' stands for. It could mean either 'Cut-out' or 'Consequence'. I further note that the left to right syntax in alarm list messages does not follow a coherent and meaningful structure. For example, the column entitled 'Alarm' should read 'Threshold'.

642 Unacknowledged and Cleared alarms are shown in reverse video (coloured background with black text), whereas acknowledged alarms are shown in normal video (coloured text on a black background). Colour-coding is used to distinguish the alarm priorities with red, orange and yellow used for alarm priorities 1, 2 and 3 respectively, and cyan used for operator defined alarms.

> ***AF-AP1000-HF-66*** *- The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.*

643 I consider that the contrast between the text and the background in alarm lists could cause legibility problems, and needs further assessment to ensure that the text remains legible in all combinations of text and background colours.

> ***AF-AP1000-HF-74*** *- The licensee shall review the contrast between the text and background in alarm lists to ensure legibility. This should specifically be included in the V&V.*

644 Unlike the alarm tiles, there is no flashing on the alarm list items. The handling status of the alarm is only indicated by the colour of the text and background as described above, but also there is an indication in the status column of the alarm list, which defines the alarm as being new, acknowledged or cleared. The description of 'CLEAR' in this column means that the parameter is no longer in alarm, and if the user resets these alarms, they will be cleared (disappear) from the alarm list.

645 I conclude that alarm list behaviours are dynamically inconsistent with that of tiles and also with standard UK practice where an unhandled (unacknowledged or unable to be reset) alarm line should flash. This should be reconsidered for the UK design.

> ***AF-AP1000-HF-75*** *- The licensee shall reconfigure the alarm list behaviours; recognising standard UK practice where an unhandled alarm line should flash.*

646 Associated suppressed alarms can be identified from the alarm tiles. If an alarm tile has one or more associated alarms that have been suppressed, the text in the alarm tile will be presented in italics. Clicking the tile allows access to the suppressed alarms.

647 Points that are on the Shelved, Nuisance or Consequent alarm lists are still in alarm, but are presented in three separate alarm lists by the workstation client. The alarm server provides a 'snooze alarm' that reminds an operator about shelved alarms after a user-configurable period of time. The operator can choose to continue shelving the alarm or move the alarm back to the current alarm list. I consider the presentation of suppressed alarms to be appropriate in principle. However, it is not clear whether new users logging on are prompted to confirm that they are aware of the alarm suppressed function, and therefore further detail is required. This also has the potential to become an onerous task during a shift handover.

> ***AF-AP1000-HF-76*** *- The licensee shall substantiate how operators will confirm their awareness of suppressed alarms particularly during shift handovers.*

648 Alarm systems are a complex design proposition. I consider that in the generic design, Westinghouse may have oversubscribed to the concept of using the alarm system to make diagnoses rather than using the alarm system as a means to prompt the need for a diagnosis. This difference may appear subtle, but it results in a distinct corresponding difference in operator activity. In the former case, the alarm system is interrogated in an attempt to make a diagnosis; which can only be entirely successful when a fault is confined to a single piece of equipment. However, when a major multi-system fault occurs with cascade effects, then the alarm system can only indicate the need to the operators to interrogate the status of the plant and its safety critical indications in order to make an appropriate diagnosis by means of procedures. For such key faults it will be necessary to justify the number of alarms and other indications that will be present and to assess the impact of this on operator response.

649 Therefore, my overall judgement is that the alarm system requires further consideration, both in the definition of the alarm population and its dynamic behaviour and also in the functionality and HF characteristics of the user interfaces.

4.6.6 Engineering Tests

650 Westinghouse undertook a series of three engineering tests to trial specific aspects of the MCR design; The Phase 1 test focused on the soft control design; Phase 2 considered the team structure within the MCR (specifically 2 and 3 person teams) and the Phase 3 trial focused on elements of the DCIS, PDSP, system presentation of reactor parameters, the WPIS and the CPS system and alarms.

651 In judging the adequacy of these tests, I first consider the analysis process. I consider that the analysis was well planned and that the methods used were selected appropriately to provide a comprehensive assessment of the soft controls. The operators appeared to be representative of the operating crews who would be operating AP1000, apart from the fact that their training had not been as thorough.

652 The engineering test 1 included an observation based error analysis while the operators were undertaking their tasks. This facilitated the identification of some of the areas where additional training would be beneficial. The analysis of the errors was also reinforced by the link analyses.

653 It would have been helpful to have included a reference to the National Aeronautics and Space Administration (NASA) Task Load Index (TLX) approach that was used in the study. I note that the current tendency in the UK when using NASA TLX is to calculate a weighted value from six rating scales, although Westinghouse calculated the unweighted

mean from eight ratings. However, this is a minor point and Westinghouse's workload assessments do appear to have been undertaken correctly. Therefore, I conclude that the data presentation in the report is adequate.

654 I note that whilst the study revealed several design issues that could be applied more widely throughout the design, it was limited to the two scenarios.

655 With regard to engineering test phase 2, I note that the difference in performance and subjective workload assessments between two-person and three-person operation were generally relatively limited. To some extent, this may have been because the tests using the two-person teams were performed after those using the same persons in three-person teams. It is therefore possible that there was some confounding between the effects of team size and experience on the particular scenarios. However, the two-person teams did not experience any difficulties. The subjective workload measures from the individual team members indicated that workload was generally a little lower than it was for the Phase 1 tests, but this was explained by the increased number of screens and other improvements that had been implemented since the Phase 1 tests. The differences in perceived workload for the individual workload factors between two-person and three-person teams were small, apart from the communication workload, which was approximately 15% higher for the three person teams, and was the highest rated of all the eight workload scales. I consider that the increased communication workload found in this scenario may suggest that in higher overall workload situations, inter team communication requirements could, to some extent, reduce the advantages of task sharing.

656 I consider that the Phase 2 tests provided Westinghouse with useful information that was well presented, with clear explanations of the limitations and specific suggestions for improvements to the design of various aspects of operations within the MCR. I also consider that this was a well planned and executed study that met all of my criteria for assessing the task analysis process and the presentation of task analysis data.

657 The Phase 3 Tests were an extension of the previous Phase 1 and 2 Tests; undertaken in an updated simulator that incorporated extended modelling of the plant parameters and the inclusion of additional interfaces; most notably the PDSP.

658 My impression of the Phase 3 tests is consistent with my previous comments on the earlier phases; in that these tests appear to have been well conceived, executed and reported. I am confident that they have produced valuable design information.

659 My only point of note is that by using unweighted NASA TLX scores, the impression could be given that the overall workload was below the normally acceptable range. From the results for all eight workload scales (which are also presented), I consider that the workload assessments are acceptable.

660 At the start of the Engineering Trials Westinghouse had identified 83 design issues of concern (Ref. 110), and these were progressively reduced as a result of the trials to 28 outstanding issues at the end of Phase 3. The 28 were then entered into Westinghouse's HF tracking system for action. This gives me some confidence that Westinghouse was using these trials to actively improve the design.

4.6.7 Procedures

661 These findings relate to item (5) from the methodology and scope presented in section 2.2.6.1.

662 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. The procedures design system is also integral to the operational concept underpinning the HRA. My assessment is therefore limited to the format and presentation of the procedures, to inform my judgement on their ability to underpin the GDA risk assessment.

663 The main operational documentation for AP1000 is a comprehensive set of procedures that are intended to provide written instructions for all predictable operational and maintenance tasks that may be necessary. These procedures will include:

- Normal Operating Procedures (NOPs);
- AOPs;
- EOPs;
- Alarm Response Procedures (ARPs);
- Severe accident management guidelines;
- Surveillance test procedures; and
- Maintenance procedures.

664 There will also be other operational documentation required, such as administrative controls and technical specifications, as the safety case moves forward.

665 Westinghouse has developed a computer-based system for the presentation of procedural information known as the Computerised Procedure System (CPS), and this can be used to present some of the procedures on the DCIS.

666 In the December 2009 PCSR (Ref. 17) Westinghouse highlights the important role of the procedures and states that *"In the event of faults the operators are guided by symptom-based procedures to place and maintain the plant in a safe and controlled state"*. This claim on the use of procedures to respond effectively to fault situations is also repeated in the UK HF Safety Case (Ref. 35) which claims that the operators will *"Perform emergency procedures to mitigate accidents, including monitoring and maintenance of the critical safety functions"*.

Emergency and Abnormal Procedures

667 Westinghouse explain that the EOPs and AOPs would normally be presented on the CPS, and in the UK HF Safety Case (Ref. 35) it summarises how the CPS will be used for these procedures, by stating that *"The CPS assists the operators in monitoring and controlling the execution of procedures. The CPS is accessible via the VDU-based workstations and provides navigation links to the non-safety control system. The CPS automatically assesses and presents the status of each step and automatically executes parallel monitoring, alerting the operator to such information when it needs attention"*.

668 An overview description of the CPS is provided in Ref. 77.

669 I consider that the main display pages provided on the CPS are relatively clear and they provide sufficient information about each step to enable the operators to complete their checks or remedial actions effectively. The Flow Chart View provides sufficient information for the operators to develop effective mental models of the required tasks. However, I consider that this display would be strengthened if a hierarchical approach was taken (as required by NUREG 0700, section 8.1.5-1 (Ref. 10)) to the main tasks, as this

would help the operators to divide the overall task into manageable perceptual chunks, whilst also focusing in more detail on their immediate tasks.

> ***AF-AP1000-HF-77*** *- The licensee shall consider presenting the main tasks or task subsets on CPS displayed procedures hierarchically, to help the operators to divide the overall task into manageable perceptual chunks, whilst also focusing in more detail on their immediate tasks; or justify the existing design.*

670 Although the Step Detail View showed identical text to that provided on the paper procedures, there were differences between the two media in the way that this information was shown. I consider that the format and layout of these pages on the CPS is much clearer than it is on the paper procedures. I also consider that the Logic Displays provide a very effective summary of the plant conditions. These will be helpful in diagnosing the underlying issues at any particular step, and possibly may provide some useful cues if an inappropriate procedure has been entered.

671 I was particularly impressed by the Parallel Information facility. This appears to provide a good solution to what I consider to be one of the operator's most difficult tasks; continuing to effectively monitor other parameters whilst working through a highly proceduralised set of sequential tasks that demand attention. However, I consider that the value of this feature relies upon the cues for operator intervention being sufficiently attention-getting. Unfortunately, I did not have any details of how the operators would be alerted, hence I am unable to judge whether the cues will be sufficiently alerting.

> ***AF-AP1000-HF-78*** *- The licensee shall provide justification of the means by which operators are alerted by the Parallel Information facility.*

672 Navigation through the successive steps was very simple, although this is not always positive, as the navigation between displays also acts as a surrogate checklist entry that could be used for place keeping and ensuring that steps are not missed. As such, I consider that this process was too simple, such that there is a potential to inadvertently click past a step, be diverted, and then moving directly to the next step without completing the previous one, or intentionally clicking past several steps without adequately checking them, as expectations of problems in a sequence are low. I have previously identified this concern in my Work Stream 1 assessment as a potential source of human error.

> ***AF-AP1000-HF-06*** *- The licensee shall assess the quality of checklists available in terms of their support to human reliability; and consider the use of items 1 and 2 of THERP Table 20-7 to model errors of omission.*

> ***AF-AP1000-HF-79*** *- The licensee shall ensure that the CPS incorporates design features to prevent operators from bypassing safety significant procedural steps, or justify the existing design.*

673 I also accept that there are similar problems with poorly designed checklists, which incorporate too many items, often for relatively trivial or straightforward tasks. In both cases, I consider the solution to be the incorporation of a more limited number of check steps at critical points.

674 In terms of the CPS displays, I consider that the ticks and crosses that are displayed provide an additional opportunity to scan previous steps very quickly as a check at any point. However, I also consider that little reliance can be placed on the operators always undertaking such a check, as there will be a bias towards thinking that all steps have been

completed. Therefore, I recommend that consideration be given to inserting effective checksteps at particular points that require a more positive response. For instance, an operator could be required to confirm whether a set of the previous steps were now completed, by entering a specific character on the keyboard.

> ***AF-AP1000-HF-80*** *- The licensee shall reconsider and justify the checking regime on the CPS displays.*

675 Regarding the ticks and crosses, it could be argued that the use of green to indicate that conditions have been fulfilled is incompatible with the colour-coding that is used elsewhere in the DCIS, where green is associated with a *'Closed'* or *'Off'* state. Therefore, for example, if a procedural step involved a check that a set of valves were all open, there would be a conflict between a green tick and the usual colour-coding for a closed valve, which is red. However, if the coding is perceived as relating to the energetic state of the procedural step, then green colour-coding for the ticks would be appropriate as the conditions would be fulfilled. In any event, for this particular situation, I consider that the icons themselves provide the strongest cue, such that there is little potential for these conditions being misinterpreted by the operators, even under potentially stressful conditions.

676 I consider that Westinghouse has been very comprehensive in providing additional information sources for the CPS users. The Graphics tab is particularly useful, but I was unable to confirm whether this is updated to reflect the potential requirements for the currently selected step. I suspect that most of the additional information that can be accessed from the Documents tab will not be used in an actual event, but this does not detract from it – it is available, and it will be valuable for training purposes.

677 With regard to the paper-based versions of these procedures, I consider that the Guidelines for Two Column Procedures (Ref. 144) provide some useful recommendations for the wording and structure of the instructions, but there are additional points that are omitted. In particular, I consider that Section 5.8.3 on the use of acronyms and abbreviations should have included statements about minimising the use of acronyms and abbreviations, and avoiding the use of conceptually meaningless codes. To assess how well the guidelines have been implemented, I examined three procedures against selected guidelines, and in all cases the procedures met the guidelines.

678 I have minor issues relating to the format and layout of the paper based procedures; for example there is a lack of typographic and presentation cues to structure the procedural information to aid assimilation and draw attention to key information. Furthermore to minimise opportunity for confusion, particularly if a need arises to switch to paper based procedures these should align closely in style, format and content with those presented on the CPS.

> ***AF-AP1000-HF-81*** *– The licensee shall provide a justification for the effective and reliable transition between the CPS and paper based procedures in the event of a failure of the CPS.*

> ***AF-AP1000-HF-82*** *– The licensee shall provide Computer based and paper based procedures of a similar format, style and structure to minimise opportunity for confusion or justify an alternate approach.*

679 There was also a lack of a hierarchical structure to the main steps. Arranging the main steps hierarchically into groups of related steps enables the operators to obtain a good overview of the main tasks, whilst also providing a more detailed impression of the group

of tasks that are the current focus of attention. In this way, the operators can build up effective mental models of the tasks and their progress through them. This process of developing and maintaining appropriate mental models is supported if the tasks are arranged in manageable chunks of up to eight or nine main tasks.

680 There are 44 tasks listed for EOP E-0; and it is difficult to assimilate this number of tasks mentally. If these had been grouped into six or seven sets of related tasks, it would have been relatively straightforward to develop an effective overview of the way that these contributed to achieving the overall goal of E-0. Similarly, whilst working through the procedure, it would be much easier to understand how the current task related to the more immediate sub-function, than to relate all 44 tasks to the achievement of the overall functional goal.

681 The two column arrangement could result in confusion; as items in the Response not obtained column are all vertically aligned with the first item in the left-hand column. Hence, when there is more than one item in the left-hand column, it is not always clear whether all the remedial actions apply singularly or collectively.

682 I note that Westinghouse avoid the use of long sections of instructional text, and that each component to be checked or operated was listed on a separate line, thereby reducing the risk of missing an item.

683 The guidance also suggests the application of simple sentence structures with information presented in standard ways. However, in the procedures that I examined I found that many of the instructions had become fragmented and without verbs; rendering the instructions more difficult to assimilate.

684 I note the overuse of acronyms and abbreviations in general and for system designator codes in particular. In written procedures, the only reason to use anything apart from the full wording is when labels are referred to, and even then the full text description should also be provided. Yet I found examples of acronyms being expanded into text that still included abbreviations.

685 However, my primary issue relates to the use of system designator codes and whilst this is of particular relevance for the procedures, the high use of system designators also impacts the use of most displays. These system designators are generally presented as three letter codes in upper case characters. This format minimises the cues that would otherwise be available from the overall patterns presented by item descriptions provided as full text in upper and lower case characters. Therefore, it impedes visual search. Once these codes have been read from procedures, it is necessary for operators to then rely upon memory to properly identify the item concerned. Sometimes the codes include useful cues, but often they do not and there are many cases where the code can be misinterpreted due to the similarity to another acronym. For example, according to the procedure writing guidelines, SMS is the code for the Special Monitoring System, but the code for the Seismic Monitoring System is SMJ. I consider that the high usage of system designator codes presents a potential increase in the human error potential, or delays when operators are working under stressful conditions.

> ***AF-AP1000-HF-83*** *- The licensee shall justify or remove the high usage of system designator codes in procedural information.*

686 However, I was pleased to note that within these procedures, references to specific plant items started with text descriptions that were then followed by the item identification codes. This use of text descriptions rather than reliance upon the item identification codes should help to reduce item identification errors.

687 In general I consider that the CPS presentation of procedures generally meet relevant criteria, although I note issues relating to place keeping.

688 Apart from my principal concern relating to the use of system designators, the paper-based procedures meet my criteria for the level of detail provided and the wording of instructions, although in other respects they were poor. In particular, I did not consider that the procedures were presented in a way that would assist operators to develop effective mental models of their tasks, which increases the potential that actions may be undertaken by rote, rather than by understanding. Regarding place keeping and reducing the potential of omitting steps, I considered that the printed procedures were acceptable, but that there was room for improvement. I consider that Westinghouse's proposal that the operators will mark paper copies of the procedures as a place keeping check is completely inadequate.

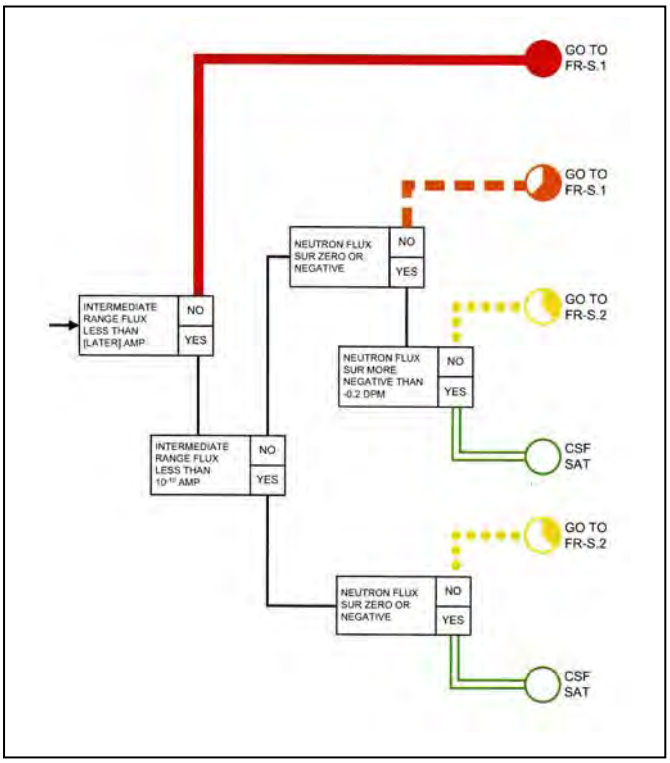
> ***AF-AP1000-HF-84*** *- The licensee shall provide and justify a place keeping system / methodology for procedural use that does not rely on operators marking up paper copies of computerised procedures.*

689 As noted earlier; EOPs will be provided via the CPS, with paper versions available within the MCR should they be required (in the event of CPS failure for example). However Westinghouse have not provided a justification as to how such a transfer will be managed reliably.

> ***AF-AP1000-HF-81*** *- The licensee shall provide a justification for the effective and reliable transition between the CPS and paper based procedures in the event of a failure of the CPS.*

690 The monitoring of the six AP1000 CSFs and manual initiation of any associated CSFs are designated as Emergency Operating Functions, and as such they are displayed on the CPS. According to the CSF monitoring procedure (Ref. 145) for an operating reactor, there are four points within EOP E-0 from which an operator is directed to enter the CSF monitoring procedure. This procedure provides a separate graphic display for each CSF which is used to monitor that CSF. I have only seen the CPS display for Sub-criticality, which I assume is shown as a List Detail View. I have presented an example of this CSF status tree from the printed version of EOP E-0 as Figure 2. The only difference between this and the corresponding CPS display is that the boxes on the CPS display and the corresponding response squares between the entry point and the most serious current condition will be shaded.

Figure 2: Critical Safety Function Display for Sub-criticality



691 The significance of the CSF challenge is colour-coded from green, which is acceptable, via yellow and then orange through to red, which represents the most serious challenge. The named colours that have been chosen have an intuitive interpretation which is in line with traffic light usage, but the shades of the colours themselves could be difficult for some STAs to differentiate. However, I consider that Westinghouse has supported the colour coding with two other types of coding, based upon line style (which is actually a combination of line thickness and continuity: becoming more prominent with severity) and the amount of fill in a circular symbol (becoming fuller with increasing severity). Both of these are clear and their relative importance is intuitive; hence I consider that the coding is well implemented.

692 In an accident situation, the STA will regularly monitor all of the CSF status trees and will first deal with the most serious condition, by entering another EOP as directed. When the reactor is at Cold Shutdown there is a similar CSF monitoring process that can be undertaken (Ref. 146), but this has only one status tree on which there are seven conditions (all orange) which could require action.

693 I have examined the paper versions of several of these CSF procedures (e.g. Ref. 147) and found them identical in format to the other EOPs, with the same attendant issues. Therefore, in this section my assessment will focus on the status trees.

694 I assume that the individual CSF recovery procedures will be presented in a similar way to the other procedures on the CPS, apart from the fact that there will be a separate tab for the appropriate CSF status trees.

695 The only substantive difference between the CSF procedures and the other EOPs is the status tree display format; which I found simple to interrogate and use. My only slight reservation was that I could not see a clear navigation tab to move to the appropriate remedial procedure; although this is rectifiable.

Alarm Response Procedures (ARPs)

696 Westinghouse claim that the ARPs provide procedural support to assist the operators in diagnosing and dealing with all alarms. As the UK HF Safety Case (Ref. 35) states *"the RO responds to alarms promptly and in accordance with the ARPs"*. Elsewhere in the same document Westinghouse states that *"Each alarm is provided with an associated ARP and on acknowledgement of the alarm; the operator will open the ARP and follow the procedure steps"*, which suggests that ARPs will be available for all alarms and that they will always be used. This view is reinforced by a statement that *"The ARPs provide step by step instructions to operators on how to respond and recover from an alarm"*.

697 My assessment of the ARPs is based upon examination of the ARPs for the Passive Containment Cooling System (PCS) (Ref. 148) and the Reactor Coolant System (RCS) (Ref. 149). I examined paper copies of these documents, but I understand that this information will usually be accessed electronically from the alarm lists. Clicking on a poke within a displayed alarm line will take the user into the procedure associated with that alarm.

698 On entering the alarm procedure from the alarm list, it appears that the most effective way to locate a specific alarm will be via the coded alarm point identifier. However, there will typically be a large number of alarms associated with a system, therefore locating the correct identifier will take time, and it also introduces the potential that an incorrect identifier and alarm response will be selected. There is also the potential that after selecting the correct alarm response from the index, the operator may navigate to an incorrect page. This potential would be eliminated if selection of the initial alarm message directed an operator to the procedural steps for that particular alarm, but I have no information about the mechanism for selecting and displaying the ARPs.

699 At this stage in the development of the ARPs, many of the alarm threshold values have not been determined, but where they have, I considered that excessive use appears to have been made of percentage of measurement range, rather than process values expressed in engineering units. The potential underuse of engineering units should be re-examined to ensure that measurements are meaningful to operators.

> ***AF-AP1000-HF-85*** *- The licensee shall reassess the alarm threshold values in terms of their meaningfulness to operators and the application of standard engineering units rather than percentage of measurement ranges.*

700 I found that the procedural information was unnecessarily terse and heavily reliant upon the use of equipment identification codes and abbreviations, rather than text descriptions and complete words. Therefore the instructions were difficult to interpret and follow. There was also a lack of directive guidance regarding appropriate remedial actions. For example, in one of the responses the operator is directed to check the *"PCCAWST water temperature"*, but no guidance is provided regarding what this should be.

701 After examining the guidance for over a hundred specific alarms, I am left with the impression that the ARP provides little additional information and guidance to that which an experienced operator would obtain from a well constructed alarm message. I also note that there are relatively few references to the requirements to rectify the underlying problem and the permitted timescales for doing that. I consider that it would have been very helpful to have referred to specific Technical Specifications at the end of many of the procedures, in order to provide guidance about post-alarm maintenance priorities; and this should be considered by a prospective licensee going forward.

AF-AP1000-HF-86 *- The licensee shall consider operator support requirements relating to rectifying underlying problems associated with alarm messages and the permitted timescales for doing that.*

702 I conclude that the ARPs do not meet my assessment criteria and that Westinghouse's claims for them are not met.

Other Procedures

703 All the other procedures will be produced to a free text format that includes checkboxes and spaces for recording specific information. These procedures will be paper–based.

704 The Normal Operating Procedures (NOPs) comprise both a set of general operating procedures that enable the *RO*s to change the operating modes for the reactor, and system operating procedures which provide guidance on system-specific tasks. These procedures are only used in paper format. They are produced in a hierarchical format that incorporates checkboxes against some items and spaces for recording particular data.

705 Apart from the above features, the guidelines for the producing NOPs (Ref. 152) were similar to those already described for the two column procedures.

706 The instructions for writing Maintenance Procedures (Refs 153 and 154) appeared to be relatively similar to those for NOPs, but I was not able to examine any actual procedures. I was also unable to examine any of the other types of procedural information.

707 I consider that the format of the NOPs and the Maintenance Procedures meet my criteria for the level of detail provided, the wording of instructions and the provision of aids to place keeping. I also consider that the procedures were adequate in terms of the provisions made for checking, but that the effectiveness of these checks could be improved by focusing on most important checks. I also consider that it would be more useful to produce the check items and to record data on a separate checksheet rather than to have these items integral to the procedure. This would also make it easier to review the procedure and confirm that all the checks had been undertaken.

4.6.7.1 Conclusions

708 In general I consider that a comprehensive suite of procedures are provided to support operator reliability. I note largely minor points of design that should be considered and remedied by a prospective licensee as the procedure system is further developed. At this stage I have no significant issues relating to the procedure system that would undermine the HRA significantly.

4.6.8 Staffing and Work Organisation

709 These findings relate to item (6) from the methodology and scope presented in Section 2.2.9.1.

710 I recognise that the specifics of the staffing levels and work organisation are primarily an issue for a prospective licensee organisation. My assessment in GDA Step 4 briefly considers these issues as assumptions are made in these areas to underpin the HRA and drive the design.

711 Westinghouse has examined the MCR staffing for normal operations via the task analysis and in the engineering tests. The OSA-2 task analysis (Ref. 87) found it necessary to assign some tasks to a second *RO*, which undermines the possibility of a solution with a

single operator and a single supervisor. The staff roles and responsibilities have also been assessed for a number of situations (Ref. 155). The Phase 2 engineering test (Ref. 156) examined the two and three person teams undertaking an emergency scenario in the MCR and found that both could undertake these tasks effectively. The Phase 3 engineering test results (Ref. 143) found modest workload levels and favourable comments in this regard.

712 The staffing concept proposed by Westinghouse may not be adopted by a UK licensee; and this has been discussed extensively throughout my assessment (Sections 4.2 and 4.6 refer).

713 Westinghouse has not presented an analysis of plant staffing levels, but has used a staffing analysis for the purposes of dose estimation. I consider that a UK analysis of overall staffing in different conditions will be required as the safety case moves forward. In particular I will expect a justification of the minimum staffing levels required to support the development of the Emergency Plan for a prospective licensed site in the UK.

> ***AF-AP1000-HF-32*** *- The licensee shall provide a justification of the minimum staffing levels proposed.*

4.6.9 Conclusions

714 I consider that in general the quality of the design based HF 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) is broadly adequate and will not significantly undermine human reliability. I note many minor observations across the assessment area and these are cited as Assessment Findings to be addressed post PCSR.

715 At the time of writing there was a lack of evidence relating to communications, the approach to emergency response and TNA and this has limited the breadth of assessment anticipated by my Assessment Plan (Ref. 1).

> ***AF-AP1000-HF-87*** *– The licensee shall provide arguments and evidence relating to the HF aspects of communications, the approach to emergency response and a Training Needs Analysis.*

4.7 Overseas Regulatory Interface

4.7.1 Introduction

716 Our GDA "Strategy for Working with Overseas Regulators" is described in http://www.hse.gov.uk/newreactors/ngn04.pdf. (Ref. 168). 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.

717 Additional information is provided in our GDA publication "Safety assessment in an International Context" http://www.hse.gov.uk/newreactors/ngn05.pdf, (Ref. 169) which explains why the UK has to undertake its own safety assessment for new reactors, how we take into account international standards and the ways in which we exchange information with overseas regulators on a general basis.

718 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; and*
- *The willingness of the overseas regulator to engage with HSE on issues of primary interest to the UK, including providing access to detailed information."*

719 Our strategy notes that the prime objective of our assessment is to consider the designs against UK requirements. However, where we consider that an overseas regulator's assessment can provide substantial/significant additional assurance, as a result of its scope and rigor, then we will take this into account during our detailed assessment. Furthermore, where another regulator's assessment identifies issues of concern, then we will use this information to help us focus our assessment effort.

720 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.

721 It should be noted that there was no specific working group of the Multinational Design Evaluation Programme (MDEP) for either HFE or HRA (via HF or PSA), under the AP1000 Working Group; more information on which can be obtained via http://www.oecd-nea.org/mdep/ (Ref. 170).

722 For the HFE and HRA aspects of the AP1000 design, I consulted with regulator colleagues in the US NRC and the Canadian Nuclear Safety Commission (CNSC). A summary of the interactions and how I have taken any assessment benefit from their work is described in Sections 4.7.2 and 4.7.3.

4.7.2 US Nuclear Regulatory Commission

723 The US NRC operates an entirely different regulatory regime to that of the UK. Their administration is based on prescribed codes and standards to be followed; and against

which submissions are judged for conformance. This is in stark 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, and not applied in the US regime. However, I undertook to understand and judge the relevance of the US assessment of the HFE and the HRA to my assessment; detail of which are described below.

4.7.2.1 US Nuclear Regulatory Commission Human Factors Engineering

724 I undertook a technical meeting at the US NRC in December 2009 to exchange information on regulatory assessment strategy for the HFE aspect of the AP1000 submission. I also assessed, at a very high level, the following publicly available document:

- Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design (NUREG-1793), Chapter 18 – Human Factors Engineering http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/chapter18.pdf (Ref. 171).

725 The NRC reviewed chapter 18 'Human Factors Engineering' of the AP1000 Design Control Document' Tier 2, largely against the criteria prescribed by NUREG-0711 Human Factors Engineering Program (Ref. 54). This review contributed to the granting of the final Design Certification Rule (DCR) by the NRC in January 2006; several years before my GDA Step 3 and 4 assessments. In the intervening period Westinghouse has progressed design of the AP1000 and its supporting analyses and in particular has produced materials specific to the UK; thus limiting the relevance of the NRC review to my GDA Step 4 assessment.

726 NRC notes that the DCD Tier 2 does not include detailed methodologies, and hence detailed evaluations were not possible. Its aim appears to have been to determine whether the Westinghouse HFE program provides a top level identification of the substance of each of the NUREG 0711 criterion, such that after design certification, the criteria will be developed into a detailed implementation plan. This is cited as a 'programmatic review'. In addition the NRC undertook 'implementation plan reviews', and 'complete element reviews' of specific aspects of the Westinghouse submission. It did not appear however that the NRC had carried out a detailed assessment of the actual analytical evidence base to underpin the safety case for the AP1000 from a HF perspective.

727 I reviewed the (European) DCD from a HF perspective as part of my GDA Step 3 assessment (Ref. 6), and deemed the material largely inadequate for UK regulatory requirements. As a result Westinghouse developed a HF safety case for the UK, which has formed the basis of my assessment for GDA Step 4. Therefore the submissions assessed by myself and the NRC are not aligned; although the UK safety case does draw upon some fundamental analysis that underpinned the USA submission. In addition, the assessment base that I have applied (UK SAPs and TAGs) is not entirely aligned with the US assessment base (NUREG 0711) in both scope and assessment approach. I did however explicitly build in a comparison between NUREG-0711 criteria and the UK SAPs into my Work Stream 4 (HFI) scope.

728 One area where I have taken advantage of NRC assessment findings is in relation to the Westinghouse functional based task analysis and operational sequence analysis. The NRC review commented that these analyses provide *"a particularly strong technical basis for identifying operational requirements to be addressed in the detailed HSI design."*

4.7.2.2 US Nuclear Regulatory Commission Human Reliability Assessment

Introduction

729 I commissioned one of my TSCs to undertake a review of the applicability of the NRC assessment of the Westinghouse HRA to the UK. The TSC involved with this work is a former NRC Senior Level Advisor on PSA/PRA and HRA, and a recognised world expert in the field of HRA and PSA/PRA. Therefore the level of detail describing my consideration of the NRC HRA assessment is significantly greater than that of the NRC HFE review, or the CNSC HFE review.

730 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 PSAs/PRAs used to support the design certification applications, since that is where the technical review of the HRA was conducted. However, some information relevant to the HRA is contained in documentation of the review of the HFE. The principal documents reviewed were:

- NUREG-1521 – Volume 2 Chapters 15 – 24, Final Safety Evaluation Report Related to Certification of the AP600 Standard Design, Docket No. 52-003 – dated 1998, ADAMS Accession # ML070080098 (Ref. 60).
- NUREG-1793, Volume 2, Part 2 Safety Evaluation Report for AP1000, Chapter 18, 2004, ADAMS Accession # ML043450290 (Ref. 61).
- NUREG-1793 Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design. Chapter 18, Docket No. 52-006, Supplement 2. ADAMS Accession # ML1120612310 (Ref. 62).
- WCAP-16555, APP-GW-GLR-011, Rev. 0, AP1000 Identification of Critical Human Actions and Risk Important Tasks, 2006. (Ref. 63).

Background to the NRC HRA Review

731 The NRC review of the AP600 and AP1000 have been performed over a number of years, during which the time the tools available to support reviews of PSAs/PRAs have changed significantly in the USA. Notably the ASME/ANS PRA standards (Refs 48, 51 and 53) and RG 1.200 (Ref. 49) have been published. The early reviews of the AP600 and AP1000 design certification submittals were completed before these documents were in routine use. NRC relied heavily on the AP600 review for the AP1000 review, but the AP600 material is too old for it to be available in the Agencywide Documents Access and Management System8 (ADAMS). Current NRC review of a PRA for new reactors is guided by SRP19.0 (Ref. 50) which addresses PRA quality, including HRA, by invoking RG 1.200 (Ref. 49), which in turn endorses the ASME/ANS PRA standard (Ref. 48). The AP600 review was performed before these documents were published, and so was the initial Final Safety Evaluation Report (FSER) for the AP1000 submittal.

732 The NRC staff reviews of the PRAs were primarily performed to assess whether the PRA models were adequate to identify insights that could be used for the licensing of the plant or for finalising the design. As stated in the AP600 and AP1000 Safety Evaluation Reports (SERs) (Refs 60, 61 and 62): *"(t)he general objectives of the NRC staff's review of the AP600/AP1000 design PRA included the following activities:*

[8] ADAMS is the official recordkeeping system of the NRC. It provides general access to publicly available NRC documentation

- *identify safety insights based on systematic risk-based evaluations of the design;*
- *support the process used to determine whether regulatory treatment of non-safety systems (RTNSS) was necessary;*
- *determine in a quantitative manner whether the design represents a reduction in risk over existing plants;*
- *assess the balance of preventive and mitigative features of the design;*
- *assess the reasonableness of the risk estimates documented in the PRA;*
- *support design certification requirements, such as inspection, tests, analyses, and acceptance criteria (ITAACs), design reliability assurance program (D-RAP), technical specifications (TS), as well as combined operation license (COL) and interface requirements."*

733 In addition, the staff used the AP600/AP1000 PRA to determine how the risk associated with the design relates to the safety goals of CDF less than 1.0×10^{-4}/yr and LRF of less than 1.0×10^{-6}/yr, and to uncover design and operational vulnerabilities.

734 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:

- *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."*

735 A major element of the HRA is to identify and define the HFEs included in the PRA logic model. These were used by the vendor and the NRC staff to identify the critical or risk-significant human actions. The critical human actions are defined in NUREG-0711 (Ref. 54) 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 NRC staff, it appears that 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 NRC review stated above. As discussed later, since the methods used were 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.

736 In addition to the reviews of the PRAs, the HFE review performed by the NRC (refer to Section 4.10.2.2) includes the topics and general criteria of Element 6, "Human Reliability Analysis," of NUREG-0711 (Ref. 54):

"The objectives of the Human Reliability Analysis review are to ensure that:

- *the HRA activity effectively integrates the HFE program activities, as well as the PRA and risk analysis activities*
- *the applicant has addressed human error mechanisms in the design of the plant HFE (i.e., the HSIs, procedures, shift staffing and training in order to minimize the*

likelihood of personnel error and to provide for error detection and recovery capability)."

737 These HFE reviews did not address the HRA technical aspects, as that part of the HRA review is conducted as part of the staff's PRA review addressed in Section 18 of the SER (Ref. 62). The analysis results report for this HRA element of NUREG-0711 (Ref. 54) would require a completed function-based task analysis report. However, since design work would not be completed in this area until after design certification, this aspect is not within the scope of design certification. Instead, the HFE review focused on the integration of the HRA with HFE design, and specifically at an implementation plan review level.

Main conclusions of the NRC HRA review

738 The review of the HRA portion of the submittals is documented in Chapter 18.7 Element 6, Human Reliability Analysis and Chapter 19 Severe Accident Analysis of the FSER for AP600 and AP1000 (Ref. 60).

739 The NRC staff concluded that Revision 2 of WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan" (Ref. 55) is an acceptable plan. The Combined Operating License (COL) applicant referencing the certified Westinghouse design (AP600 or AP1000) is then responsible for the execution and documentation of the HRA/HFE integration / implementation plan. Section 3.0 of the plan requires the human actions and tasks identified by HRA activities to be included in the set of tasks examined using operational sequence task analyses. The analyses are to include performance requirements, such as time windows, within which an action needs to be completed. Workload of the operators should also be addressed. Section 4.0 states that any critical human action or risk important task, that is determined to be a potentially significant contributor to risk, will be re-examined by task analysis, HSI design, and procedure development. These evaluations will be used to identify changes to the operator task or the HSI to reduce the likelihood of operator error and provide for error detection and recovery capability. Section 5.0 discusses the validation of HRA performance assumptions. It states that validation of the HRA operator performance assumptions will be performed as part of the Integrated HFE system validation. This will include scenarios that include critical or risk-important human actions, as well as specific performance assumptions that the HRA/PRA group identifies for confirmation. After review of the results of the validation, the HRA/PRA group will determine whether any changes need to be made to the HRA assumptions or HRA quantification. If changes are needed, the HRA will be modified and the impact on the PRA will be assessed. A report will be generated, documenting the results of the exercises intended to validate the HRA performance assumptions, and submitted to the NRC for review as part of the COL application information provided in COL Action Item 18.7-1.

740 In the technical area of HRA, the PRAs have primarily been used to identify critical human actions. Essentially, what the PRAs identify is the HFEs that are included in the PRA model and that meet specified criteria with respect to their Fussel Vesely (FV) (or Risk Decrease) and Risk Achievement Worth (RAW) (or Risk Increase) importance measures. These basic events need to be interpreted to identify the associated critical operator functions. In some cases, for example, the basic events represent conditional probabilities of human failure given a prior human failure, and are not specifically related to functions. In addition, limited sensitivity studies and qualitative criteria are used to identify risk significant operator functions. These criteria are described in detail in Section 2 of Ref. 55. The NRC staff accepted that the approach to the identification and definition of these HFEs has been performed in an acceptable manner. As an example, the

AP1000 critical human actions are identified in WCAP-16555 (Ref. 63), and have been accepted by NRC (SER Chapter 19 Supplement 2, dated 13/05/2009 refers). The report not only identifies post-accident tasks, but also identifies equipment for which maintenance, surveillance, and administrative controls are needed, based on the risk-significance of the equipment to which these administrative controls would apply. Essentially this means that the NRC staff considers the PRA logic models and the approach used to identify the significant HFEs to be adequate. As indicated above, the applicant that references the certified design is responsible for demonstrating that the PRA is consistent with the as-to-be-built and operated plant.

HRA methods used in US Design Certification PRA submittals

741 The HRA method applied in Westinghouse's US application for the AP600 and AP1000 was THERP (NUREG/CR-1278 (Ref. 13)). THERP is an NRC-developed method, and hence there was no NRC staff concern with the method itself, but only with the way it was initially applied. There were concerns with the application of the HRA approach in the initial Westinghouse submittal on the AP600, but the PSA was subsequently revised to the satisfaction of the NRC reviewers (Section 19.1.1.2 of NUREG-1521 (Ref. 60)) states that the PRA quality was considered sufficient for the purpose of the Design Certification).

Relevance of NRC HRA reviews to ND's GDA

742 Based on the documentation reviewed, there appears to be little that ND can benefit from the NRC reviews of the PRAs, other than the 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 NRC. There is also little or no documentation regarding the evaluation of the application of THERP.

743 It appears that the NRC review was undertaken at a much higher level than my Work Streams 1 and 2, and performed for an entirely different aim, against a prescribed set of criteria not analogous to the goal setting criteria of our HRA TAG.

4.7.3 Canadian Nuclear Safety Commission

744 I undertook a technical meeting with the CNSC in December 2009 to exchange information on regulatory assessment strategy for the HFE aspect of the AP1000 submission.

745 In 2009 the CNSC undertook a 'pre-project design review' of the AP1000, which included a HF element. The stated scope of that assessment was a high-level review of the reactor design to determine whether Westinghouse had correctly understood CNSC's regulatory requirements with regard to HF, and whether the submitted AP1000 design documents met those regulatory expectations. The CNSC HF assessment considered a sample of clauses from their regulatory guide on the design of new nuclear power plants, within a sample of HF topic areas. The most relevant topic areas to the UK assessment are *'general aspects of HF in design'*; '*HF aspects of plant safety functions and characteristics'*; *'HF aspects of maintenance and repair'* and *'HF aspects of handling and storage of fuel…..'*. I also briefly considered the review of *'HF standards used in design'*.

746 The key Westinghouse document informing the CNSC review was the "AP1000 Human Factors Program and Assessment for Canadian Nuclear Safety Commission". I have not had sight of this report and hence I am not able to judge comparability with the UK submission. The CNSC assessment report considers the submitted documentation on a clause by clause basis and provides a judgement on whether Westinghouse has demonstrated understanding of the clause and an adequate intention to comply. This

latter point is most pertinent to my ability to take any advantage from the CNSC assessment, as their assessors were generally only seeking assurance of a forward intention to comply; rather than an evidence based demonstration of actual compliance. It is noted that the CNSC generally regarded the submission provided by Westinghouse as sufficient for the purpose of their review.

747 Essentially it appears that the CNSC review was at a much higher level than those I have undertaken, and it was for a different aim; largely as a result of their review being a 'pre-project' assessment. I consider that an equivalent to GDA Step 4 assessment would be undertaken by CNSC in their subsequent reviews at an appropriate phase of the AP1000 license review process. As a result I have not been able to take any assessment benefit from the CNSC work to date.

5 CONCLUSIONS

5.1 Overview

748 Overall, I consider that Westinghouse has undertaken a significant volume of quality HF assessment work to support their GDA submission for HF. Westinghouse has applied considerable competent resource to improve its position on HF from that at the end of GDA Step 3. My interactions with its team have been positive, and through regulatory intervention and a willingness by Westinghouse to understand the UK regulatory system and safety case regime, its achievements in HF at the end of GDA Step 4 are to be commended.

749 There are gaps in the HF safety case; some of which are significant and have resulted in a GDA Issue. However Westinghouse has delivered analyses to address these concerns; unfortunately these were delivered in November and December 2010 and I was unable to fully consider them within GDA Step 4.

750 The majority of my conclusions are cited as Assessment Findings to be taken forward as routine regulatory business post Generic PCSR. This reflects my judgement that in the HF technical area, based on my assessment, there is a minimal risk to progression of the generic PCSR. Should subsequent assessment reveal further deficiencies in the design or safety analysis, typically HF solutions can be developed an implemented without undue effect on the design of civil structures or major pressure 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.

5.2 Assessment Area Conclusions

751 In each of my assessment areas the principal conclusions are as follows.

5.2.1 Work Stream 1 - Substantiation of Human Based Safety Actions

752 In general I judge that Westinghouse has applied itself to the problem of human factors substantiation, and has identified some sources of operator failure that were omitted by the PRA. Westinghouse has captured and incorporated some valuable Utility input, together with some potentially useful error reduction strategies and some of the human based safety claims seem reasonable.

753 There are 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 AP1000 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.

754 I recognise the delivery of material that Westinghouse propose to address my regulatory observations in the areas of operator misdiagnosis, violation potential and human error mechanisms. However as I was not able to fully consider their submission in these areas within GDA Step 4, I propose a GDA Issue to reflect the significant gap in the safety submission that these analyses represent.

5.2.2 Work Stream 2 - Generic Human Reliability Assessment (HRA)

755 It is clear that there are many and considerable issues with the current AP1000 HRA. Both myself and my PSA colleague highlighted problems with the model at the end of GDA Step 3, and the work that I have undertaken during GDA Step 4 has amplified my judgement that the HRA should be fully revised. I recognise that the qualitative HF assessment work undertaken by Westinghouse to develop the HF safety case for the AP1000 has not been reflected in the HRA; and as the safety case and supporting risk assessments move forward those analyses should be fully incorporated to the revised HRA model. I question the general applicability of Technique for Human Error Rate Prediction (THERP) and early consideration should be given to the appropriateness of THERP to the revised HRA. I do not consider that the current model represents recognised good practice in terms of quantitative HRA, and that this is largely a result of the age of the model; its incompleteness and all of the modelling issues that I highlight in this report.

5.2.3 Work Stream 3 - Engineering Systems

756 In general I judge that Westinghouse has made attempts to address the human reliability aspects of maintenance; and there is evidence of analysis and design input to support its claims in this area. However there are significant gaps in the HF contribution that I am taking forward as part of GDA Issue Action HF1.A1.

5.2.4 Work Stream 4 - HF Integration (HFI)

757 In general I judge that Westinghouse has evidence of a Human Factors Engineering (HFE) programme of work but only at the level of a HF engineering scope of work, which is in itself limited by their programme and resource split into core, adjunct and peripheral elements. This split is risk based and does not take explicit account of complexity and novelty; and in my opinion this does not necessarily result in an ALARP position. 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. This is to be addressed by a prospective licensee as part of a site specific PCSR.

5.2.5 Work Stream 5 – Plant-Wide Generic HF Assessment

758 I consider that in general the quality of the design based HF 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) is adequate, and therefore likely to support to human reliability. I note many minor observations across the assessment area, and these are cited as Assessment Findings to be addressed post Generic PCSR.

759 Table 21 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 21: Assessment Findings and GDA Issues per Work Stream

Assessment Work Stream	Number of Assessment Findings	Number of GDA Issues
1	12	1
2	18	0
3	3	0
4	16	0
5	46	0

5.3 Meaningful Generic Design Assessment

760 I judge that the assessment that I have undertaken of the human contribution to safety for the AP1000 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".*

761 I consider that I have received sufficient information and have undertaken a sufficiently thorough and detailed assessment of that information.

762 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

763 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 Westinghouse position for HF against those broad expectations.

764 ***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 Westinghouse case is largely 'complete', with the exception that I have not fully assessed the adequacy of the submissions associated with regulatory observations in the areas of human error mechanisms, violation potential and operator

misdiagnosis as these arrived in November and December 2010. I also consider that to further 'complete' the case, closer reference between the revised HRA and the HFE analysis will be required.

765 ***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 have no significant issues with the Westinghouse documentation in this regard, and consider the HF safety case relatively clear. However greater synergy between the HRA and HFE will significantly aid clarity as the safety case moves forward.

766 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.

767 ***Rational:*** *"the safety case should be reasonable and sensible. It should provide cogent, cohesive and logical arguments to support the conclusions"*. I consider that the HF safety case is presented in a logical manner; the referenced evidence is linked back to the arguments supporting the stated safety claims. In general the arguments are logical; my assessment findings essentially relate to the scope and quality of the evidence cited.

768 ***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 maturity and incompleteness of the model. This has been discussed widely in my assessment.

769 ***Appropriate:*** this essentially relates to the appropriateness of the methods used to substantiate safety. I have discussed this at length in my assessment, and have questioned the validity of the THERP HRA model.

770 ***Integrated:*** *"the safety case should be holistic so that there are clear links between the safety analysis and engineering substantiation"*. This is the 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.

771 ***Current:*** this relates to the requirement to review, revise and update the safety case to maintain its currency. This is not applicable to GDA.

772 ***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.

773 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for the HF. I consider that from a HF view point, the Westinghouse AP1000 design is suitable for construction in the UK. 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

774 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

775 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 Westinghouse AP1000.* HSE-ND Assessment Plan AR 09/063. April 2010. TRIM Ref. 2009/471966.

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. January 2008. www.hse.gov.uk/nuclear/saps/saps2006.pdf.

5 *Nuclear power station generic design assessment – guidance to requesting parties.* Version 3, HSE. August 2008. www.hse.gov.uk/newreactors/ngn03.pdf.

6 *Step 3 Human Factors Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/021. November 2009. TRIM Ref. 2009/335827.

7 *ND BMS. Technical Assessment Guides:*

- *ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable).* T/AST/005 Issue 4, Revision 1. HSE. January 2009. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast005.htm.
- *Maintenance, inspection and testing of safety systems, safety related structures and components.* T/AST/009 Issue 1. HSE. November 1999. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast009.pdf.
- *Early Initiation of Safety Systems.* T/AST/010 Issue 2. HSE. July 2008. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast010.htm.
- *Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.* T/AST/051 Issue 1. May 2002. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/**tast051**.pdf.
- *Human Factors Integration.* T/AST/058 Issue 1. HSE. September 2010. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/**tast058**.htm.
- *Human Machine Interface.* T/AST/059 Issue 1. HSE. November 2010. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/**tast059**.htm.
- *Human Reliability Analysis.* T/AST/063 Issue 1. HSE. 2009. http://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, US Nuclear Regulatory Commission. 1996.

10 *Human-System Interface Design Review Guideline.* NUREG-0700, Revision 2. US Nuclear Regulatory Commission. May 2002.

11 US Nuclear Regulatory Commission Regulations: *Title 10, Code of Federal Regulations, Part 50, Domestic licensing of production and utilization facilities*.

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.* (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* NUREG/CR-1278.

14 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600721.

15 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600724.

16 *Westinghouse AP1000 - Schedule of Regulatory Issues Raised during Step 4.* HSE-ND, TRIM Ref. 2010/600725.

17 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732, Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/23759.

18 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-793, Revision A. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/23783.

19 *The Master Submission List.* UKP-GW-GLX-001 Revision 0. Westinghouse Electric Company LLC. April 2011. TRIM Ref. 2011/246930.

20 *Price H E. The Allocation of Functions in Systems*. Human Factors and Ergonomics Society. pp 33–45 Volume 27, Number 1. February 1985.

21 *Sheridan T B. (1996) Human Centered Automation: A Tutorial.* Paper presented at the EHPG Meeting of the OECD Halden Reactor Project Loen, Norway. May 1996.

22 *Pheasant S and & Haslegrave C M. (2005) Bodyspace.* 3rd Edition. CRC Press.

23 *Human Factors Design Standard (HFDS) for Acquisition of Commercial Off-The-Shelf Subsystems, Non-Developmental Items, and Developmental Systems.* US Department of Transportation, Federal Aviation Administration. DOT/FAA/CT-03/05 HF-STD-001 May 2003.

24 *Shorrock S T and Kirwan B. (2002). Development and application of a human error identification tool for air traffic control.* Applied Ergonomics 33 319-336.

25 *Rasmussen J, Pedersen O M, Carnino A, Griffon M, Mancini C and Gagnolet P. (1981). Classification system for reporting events involving human malfunctions.* Report Riso-M-2240, DK-4000. Roskilde, Riso National Laboratories, Denmark.

26 *Williams J C and Munley G A. Human error identification - a new approach.* Paper preented at PSA/PRA, Safety and Risk Assessment, IBC.. London. 3/4 December 1992.

27 *Schupp B, Basnyat S, Palanque P and Wright P. A Barrier-Approach to Inform Model-Based Design of Safety-Critical Interactive Systems.* Paper presented at 9th International Symposium of the ISSA Research Section Design process and human factors integration: Optimising company performances. Nice, France. 2006.

28 *GDA Step 4 Human Factors Assessment. AP1000 Work Stream 1: Standard Approach to Human Action Assessment*. Issue 2F. Greenstreet Berman Ltd/Synergy Consultants Ltd Consortium. September 2010. TRIM Ref..2010/519902.

29 *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice*. IAEA Safety Series No. 50-P-10. International Atomic Energy Agency, Vienna. 1995.

30 *Williams J C. A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance.* Proceedings 4th IEEE Conference on Human Factors in Power Plants. Monterey, California. pp 436-450. June 1988.

31 *Williams J C. A User Manual for the HEART Human Reliability Assessment Method.* DNV Technica Report C2547. March 1992 (Unpublished).

32 Not used.

33 *Kirwan B, Kennedy R, Taylor-Adams S and Lambert B. The Validation of Three Human Reliability Quantification Techniques – THERP, HEART and JHEDI: Part 2 -Results of Validation Exercise*. Applied Ergonomics 28, 17–25. 1997.

34 *Kirwan B, Umbers I, Edmunds G and Gibson H W. Quantifying the Unimaginable – The Case for Human Performance Limiting Values.* Paper at PSAM 9 Conference, International Conference on Probabilistic Safety Assessment and Management, Hong Kong. 2008.

35 *AP1000 Human Factors Program and Assessment for the United Kingdom*. UKP-GW-GL-042 Revision 1. Westinghouse Electric Company LLC. February 2010. TRIM Ref. 2010/93187.

36 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human factors Safety Case as Reflecting the UK AP1000 PRA Update*. UKP-GW-GL-069 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82014.

37 *United Kingdom AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA*. UKP-GW-GL-070 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82016.

38 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case as reflecting the UK AP1000 Low Power and Shutdown PRA*. UKP-GW-GL-071 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82018.

39 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults*. UKP-GW-GL-075 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/82076.

40 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Identified Non-Core Damage Human Errors with Possible Radioactive Release*. UKP-GW-GL-073 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82073.

41 *ISO/IEC 15504 Information technology - Process assessment*.

42 *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants*. NUREG/CR-6947 BNL-NUREG-79828-2008. US Nuclear Regulatory Commission. October 2008.

43 *Burns, C et al. Evaluation of Ecological Interface Design for Nuclear Process Control: Situation Awareness Effects*. IFE/HR/E-2008/007.

44 *Wood, S. Flight Crew Reliance on Automation.* CAA Paper 2004/10.

45 Highlights of the Compliance Analysis - Chapter 2 - European Utility Requirements (EUR). Volume 3 AP1000 Subset. TRIM Ref. 2011/386724.

46 *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624. Revision 1.1999.

47 *BS 31100:2008 Risk management. Code of practice*. 31 October 2008. ISBN 9780580649080.

48 *Standard for Level1/Large early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.* ASME/ANS RA-Sa-2009. Addenda to ASME/ANS RA-S-2008.

49 *An Approach for Determining the technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*. Regulatory Guide 1.200. Revision 2. US Nuclear Regulatory Commission. March 2009.

50 *Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors. Review Plan Section 19.0*. NUREG-0800. Standard Revision 2. US Nuclear Regulatory Commission. June 2007.

51 *Standard for Level1/Large early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.* ASME RA-Sb-2005.

52 *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Plant Facilities*. Volume 1: Summary and Overview. NUREG/CR-6850 Final Report. EPRI 1011989. USNRC/EPRI. September 2005.

53 *External Events PRA Methodology – an American National Standard*. American Nuclear Society. ANS/ANSI-58.21-2007.

54 *Human Factors Engineering – Program Review Model*. NUREG-0711 Revision 1. US Nuclear Regulatory Commission. February 2004.

55 *Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan*. WCAP-14651 Revision 2. 1997. Westinghouse Electric Company LLC. TRIM Ref. 2011/399492.

56 *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. NUREG/CR-4772. US Nuclear Regulatory Commission. February 1987.

57 *The SPAR-H Human Reliability Analysis Method. NUREG*/CR-6883. US NRC. August 2005.

58 Not used.

59 Not used.

60 *Final Safety Evaluation Report Related to Certification of the AP600 Standard Design*. NUREG-1512 – Volume 2 Chapters 15 – 24. US Nuclear Regulatory Commission. 1998.

61 *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design.* NUREG-1793 Volume 2, Part 2 SER for AP1000, Chapter 18. US Nuclear Regulatory Commission. 2004.

62 *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design.* Chapter 18, Docket No. 52-006, NUREG-1793, Supplement 2.

63 *AP1000 Identification of Critical Human Actions and Risk Important Tasks.* APP-GW-GLR-011. WCAP-16555 Revision 0. Westinghouse Electric Company LLC. 2006. TRIM Ref. 2011/79748.

64 *AP1000 European Design Control Document*. EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC. 2009. TRIM Ref. 2011/81804.

65 Assessment of Westinghouse Treatment of Human-based Safety Actions. Report of Initial Review of Nine Selected Operator Actions. GSB2152-13. GSB Synergy Report. 2010. TRIM Ref. 2011/385365.

66 *AP1000 Fault Schedule for the United Kingdom.* UKP-GW-GLR-003 Revision 0. Westinghouse Electric Company LLC. September 2009. TRIM Ref. 2011/82086.

67 *UK AP1000 Probabilistic Risk Assessment*. UKP-GW-GL-022 Revision 0. Westinghouse Electric Company LLC. May 2007. TRIM Ref. 2011/81984.

68 GSB2152-10 (2010) AP1000 Workstream 1: Assessment of Claims – ALARP Process Assessment. GSB/Synergy Report. TRIM Ref. 2011/0385342.

69 *Court of Appeal. Edwards vs. National Coal Board*. 1 All ER 743 (CA).1949.

70 *Emergency Operating Procedure E-3. Steam Generator Tube Rupture*. APP-GW-GJP-204 Revision 3. Westinghouse Electric Company LLC. May 2009. TRIM Ref. 2011/79658.

71 *UK Compliance Document: Section A UK Safety Case Overview*. UKP-GW-GL-710 Revision 0. Westinghouse Electric Company LLC. 2009. TRIM Ref. 2011/384432.

72 *Safe and Simple: The Genesis of the AP1000 Design.* APP-GW-GER-005 Revision 1. Westinghouse Electric Company LLC. August 2008. TRIM Ref. 2011/79651.

73 *AP1000 Design Reliability Assurance Program*. APP-GW-GRR-009 Revision 1. Westinghouse Electric Company LLC. October 2008. TRIM Ref. 2011/81414.

74 *Designer's Input for the Training of Human Factors Engineering Verification and Validation Personnel*. WCAP-14655 Revision 1. Westinghouse Electric Company LLC. August 1996. TRIM Ref. 2011/82144.

75 *Interface Protocol between HSE Nuclear Directorate / Environment Agency and Requesting Parties*. Issue 2. HSE. August 2008. TRIM Ref. 2008/41861.

76 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms*. UKP-GW-GL-076 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/82077.

77 *Step 4 Human Factors – Supporting Analysis for the Westinghouse AP1000® Reactor. ONR Assessment Report*. ONR-GDA-AR-11-033 Revision 0. TRIM Ref. 2011/57354.

78 *Step 3 Probabilistic Safety Analysis of the Westinghouse AP1000. HSE-ND Assessment Report.* AR 09/017-P. November 2009. TRIM Ref. 2010/609908.

79 *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 47 K122 425–435. ISSN: 0925-7535. 2009.

80 *Workman M. The effects of technology mediated interaction and openness in virtual team performance measures. Behaviour & Information Technology*, pp 355-365, Vol. 26, Issue 5. 2007.

81 *Parush A. An empirical evaluation of textual display configurations for supervisory tasks. Behaviour & Information Technology*, pp 225-235, Vol. 23, Issue 4. 2004.

82 *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, Vol 75. February 2002.

83 *Gertman D, Blackman, H, Marble, J, Byers, J. and Smith, C. (2005). The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883, INL/EXT-05-00509. US Nuclear Regulatory Commission. August 2005.

84 *Cepin M. DEPEND-HRA – A method for consideration of dependency in human reliability analysis. Reliability Analysis & System Safety*, pp 1452-1460, Vol 93. 2008.

85 *AP1000 Human Factors Engineering Program Plan*. APP-OCS-GBH-001 Revision 1. Westinghouse Electric Company LLC. May 2009. TRIM Ref. 2011/81521.

86 *AP1000 Local Panels and Maintainability Human Factors Engineering Assessment*. APP-OCS-JCR-001 Revision A. Westinghouse Electric Company LLC. September 2010. TRIM Ref. 2011/81539.

87 *AP1000 Operational Sequence Analysis (OSA-2) Summary Report.* APP-OCS-J1R-220 Revision B. Westinghouse Electric Company LLC. August 2009. TRIM Ref. 2011/93770.

88 *AP1000 Local Panels and Maintainability Human Factors Design Guidelines*. APP-GW-GRP-001 Revision 0. Westinghouse Electric Company LLC. February 2009. TRIM Ref. 2011/93614.

89 *BS EN 60706-2:2006*. *Maintainability of equipment. Maintainability requirements and studies during the design and development phase*. British Standard Institution (BSI). October 2006.

90 *AP1000 Human Factors Engineering Design Verification Plan.* APP-OCS-GEH-120 Revision B. Westinghouse Electric Company LLC. April 2009. TRIM Ref. 2011/93722.

91 *Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary*. APP-PV70-GER-002. Revision B. August 2010.TRIM Ref. 2011/94133.

92 *AP1000 The Incorporation of Human Factors Engineering into the Development of AP1000 Plant Procedures*. APP-OCS-GER-031 Revision A. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/93731.

93 *AP1000 Human Factors Engineering Analysis to Support Technical Support Center and Emergency Operations Facility Design*. APP-OCS-J0A-001 Revision A. Westinghouse Electric Company LLC. August 2009. TRIM Ref. 2011/93748.

94 *BS EN 60964*. *Nuclear Power Plants Control Rooms. Design*. British Standard Institution. May 2009.

95 *Ergonomic Design of Control Centres.* ISO 11064-5. 2008.

96 *Ergonomic Principles in the Design of Work Systems.* ISO 6385. 2004.

97 Ergonomics of human-system interaction: *Human-Centred Design Processes for Interactive Systems.* ISO 9241-210. 2010.

98 *Ergonomics of Human-System Interaction – Human-Centred Lifecycle Process Descriptions.* ISO/TR 18529. 2000.

99 *United Kingdom AP1000 Supplemental Information for the Human Factor Safety Case – Potential Improvements as Proposed in the ALARP Analysis. UKP-GW-GL-072 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/76107.*

100 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability*. UKP-GW-GL-074 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/82075.

101 *United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults*. UKP-GW-GL-075 Revision 5. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/76115.

102 *AP1000 Design Reference Point for UK GDA*. UKP-GW-GL-060 Revision 1. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/82003.

103 *AP1000 Pre-Construction Safety Report*. UKP-GW-GL-793 Revision A. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/23783.

104 *Analysis Phase of Systematic Approach to Training for Nuclear Plant Personnel*. IAEA-TECDOC-1170. International Atomic Energy Agency. August 2000.

105 *AP1000 Human System Interface Design Guidelines.* APP-OCS-J1-002 Revision 1. Westinghouse Electric Company LLC. July 2009. TRIM Ref. 2011/81529.

106 *AP1000 Decommissioning Summary Report*. EPS-GW-GER-012 Revision A. Westinghouse Electric Company LLC. December 2008. TRIM Ref. 2011/81749.

107 Not used.

108 *Programmatic Level Description of the AP1000 Human Factors Engineering Verification and Validation Plan*. WCAP-15860 Revision 2. Westinghouse Electric Company LLC. October 2003. TRIM Ref. 2011/93263.

109 *AP1000 Human Factors Engineering Integrated System Validation Plan.* APP-OCS-GEH-320 Revision D. Westinghouse Electric Company LLC. June 2010. TRIM Ref. 2011/93725.

110 *Man-in-the-Loop Test Plan Description*. WCAP-14396 Revision 3. US Nuclear Regulatory Commission.. November 2002.

111 *AP1000 Fuel Handling System - System Specification Document***.** APP-FHS-M3-001 Revision 0. Westinghouse Electric Company LLC. March 2010. TRIM Ref. 2011/93461.

112 *The Incorporation of Human Factors Engineering into the Development of the AP1000 Plant Training Programs*. APP-OCS-GER-041 Revision A. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/93732.

113 *AP600/AP1000 Functional Requirements Analysis and Function Allocation.* WCAP-14644-NP Revision 1. October 2008. TRIM Ref. 2011/82143.

114 Not used.

115 *A Methodology for Allocating Nuclear Power Plant Control Functions to Human and Automatic Control*. NUREG/CR3331. Washington DC: US Nuclear Regulatory Commission. 1993.

116 Not used.

117 *AP1000 Design Differences Document for Development of Emergency Response Guidelines*. APP-GW-GJR-001 Revision A. Westinghouse Electric Company LLC. September 2005. TRIM Ref. 2011/93570.

118 *AP1000 Function-Based Task Analysis Summary Report*. APP-OCS-J1A-030 Revision 0. Westinghouse Electric Company LLC. November 2009. TRIM Ref. 2011/93759.

119 *AP1000 Operational Sequence Analysis (OSA-1) Summary Report*. APP-OCS-J1R-120 Revision 0. Westinghouse Electric Company LLC. December 2006. TRIM Ref. 2011/81532.

120 *AP1000 Operational Sequence Analysis (OSA-2) Implementation Plan*. APP-OCS-J1R-210 Revision 1. Westinghouse Electric Company LLC. April 2009. TRIM Ref. 2011/93766.

121 Not used.

122 *China, United Kingdom and United States Adult Population Anthropometric Data*. WNA-CN-00118-GEN Revision 0. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/82218.

123 *Peebles L, Norris B, Adult Data: The Handbook of Adult Anthropomorphic and Strength Measurements - Data for Design Safety*. London: Department of Trade and Industry. 1998.

124 *Health Survey for England – 2008: Trend Tables.* National Health Service (NHS). 2008.

125 *AP1000 Design Specification for Control Room Consoles and Panels*. APP-JC01-Z0-001 Revision B. Westinghouse Electric Company LLC. October 2009. TRIM Ref. 2011/93667.

126 *AP1000 Main Control Area Layout Top View*. APP-JC01-V1-001 Revision E. Westinghouse Electric Company LLC. February 2008. TRIM Ref. 2011/93648.

127 *AP1000 Senior Reactor Operator Console Outline*. APP-JC01-V1-200 Revision B. Westinghouse Electric Company LLC. September 2007. TRIM Ref. 2011/93653.

128 *AP1000 Reactor Operator Console (A) Outline*. APP-JC01-V1-250 Revision B. Westinghouse Electric Company LLC. September 2007. TRIM Ref. 2011/93654.

129 *Report on AP1000 Main Control Area Workshop*. APP OCS GGR 105 Revision 0. Westinghouse Electric Company LLC. March 2007. TRIM Ref. 2011/93743.

130 *Van Cott, H P and Kinkade R G. Human Engineering Guide to Equipment Design.* American Institutes for Research, Washington, DC. John Wiley & Sons, 3rd Revised edition. March 1984. ISBN-10: 0471800112 ISBN-13: 978-0471800118.

131 *Radiologically Controlled Area Ventilation System Specification Document*. APP-VAS-M3-001 Revision D. Westinghouse Electric Company LLC. May 2008. TRIM Ref. 2011/81689.

132 *Kroemer K.H.E. and Grandjean E. Fitting the Task to the Human.* London: Taylor and Francis. July 2001.

133 *Main Control Room Emergency Habitability System, System Specification Document*. APP-VES-M3-001 Revision 0. Westinghouse Electric Company LLC. May 2008. TRIM Ref. 2011/94525.

134 *Evaluation of the Noise in the AP1000 Main Control Room*. APP-12401-GER-001 Revision 0. Westinghouse Electric Company LLC. July 2007.TRIM Ref. 2011/79132.

135 *AP1000 I&C System Design Specification*. APP-GW-J4-001 Revision 1. Westinghouse Electric Company LLC. September 2009. TRIM Ref. 2011/76349.

136 *AP1000 Protection and Safety Monitoring System Software Design Description for the Safety Display.* APP-PMS-GHY-009 Revision A. Westinghouse Electric Company LLC. November 2009. TRIM Ref. 2011/93962.

137 *UK Nuclear Worker Stereotypical Representation Relative to Westinghouse AP1000 Nuclear Plant Human Factors Design*. Combined Phase 1 & 2 Report. CCD/1049/REP/002/10 Version 3. 2010. CCD Report. TRIM Ref. 2011/386755

138 *AP1000 Specification of Static and Dynamic Elements for Display*. APP-DDS-J4V-002, Revision D. Westinghouse Electric Company LLC. May 2008. TRIM Ref. 2011/93459.

139 *AP1000 Wall Panel Information System Hardware Design Specification*. APP-OCS-J4-002 Revision A. Westinghouse Electric Company LLC. August 2009. TRIM Ref. 2011/93773.

140 *AP1000 Concept of Operation*. APP-OCS-GJR-002 Revision B. Westinghouse Electric Company LLC. February 2008. TRIM Ref. 2011/93746.

141 *RRAS Distributed Control & Information Systems - Standard Alarm Presentation System Functional Requirements*. WNA-DS-01045-GEN Revision 1. Westinghouse Electric Company LLC. February 2009. TRIM Ref. 2011/82224.

142 *EEMUA Publication 191. Alarm Systems - A Guide to Design, Management and Procurement.* Engineering Equipment Manufacturers and Users' Association, London. November 2007.

143 *AP1000 Human Factors Engineering Test Phase 3 Report*. APP-OCS-T2R-030 Revision 0. Westinghouse Electric Company LLC. February 2009. TRIM Ref. 2011/81542.

144 *Writer's Guideline for Two Column Procedures*. APP-GW-GJP-200 Revision G. Westinghouse Electric Company LLC. March 2009. TRIM Ref. 2011/93564.

145 *Critical Safety Function Status Trees*. APP-GW-GJP-250 Revision 1. Westinghouse Electric Company LLC. November 2008.TRIM Ref. 2011/93566.

146 *Shutdown Critical Safety Function Status Tree*. APP-GW-GJP-230 Revision 1. Westinghouse Electric Company LLC. November 2008. TRIM Ref. 2011/79686.

147 *Response to Inadequate Core Cooling*. APP-GW-GJP-210 Revision 2. Westinghouse Electric Company LLC. October 2008. TRIM Ref. 2011/79664.

148 *Alarm Response – Passive Containment Cooling System.* APP-PCS-GJP-401 Revision A. Westinghouse Electric Company LLC. July 2009. TRIM Ref. 2011/93802.

149 *Alarm Response Procedure – Reactor Coolant System*. APP-RCS-GJP-401 Revision A. Westinghouse Electric Company LLC. July 2009. TRIM Ref. 2011/94206.

150 *Plant Heatup from Mode 4 to Normal Operating Temperature*. APP-GW-GJP-107 Revision D. Westinghouse Electric Company LLC. February 2009. TRIM Ref. 2011/93561.

151 *Plant Startup from Normal Operating Temperature to Less than 5% Power. APP*-GW-GJP-108 Revision C. Westinghouse Electric Company LLC. May 2009. TRIM Ref. 2011/93563.

152 *AP1000 Normal Operating Procedures (NOP) Writer's Guideline*. APP-GW-GJP-100 Revision G. Westinghouse Electric Company LLC. August 2007. TRIM Ref. 2011/93560.

153 *AP1000 Maintenance, Test, Inspection and Surveillance (MTIS) Writer's Guideline*. APP-GW-GJP-800 Revision A. Westinghouse Electric Company LLC. July 2008. TRIM Ref. 2011/79739.

154 *Plant Operations, Surveillance, and Maintenance Procedures*. APP-GW-GLR-040 Revision 1. Westinghouse Electric Company LLC. August 2007. TRIM Ref. 2011/93595.

155 *Designer's Input to Determination of the AP600 Main Control Room Staffing Level*. Revision 0. WCAP 14694. Westinghouse Electric Company LLC. July 1996. TRIM Ref. 2011/473979

156 *Phase 2 Engineering Test Plan for AP1000 Control Room Integration*. APP-OCS-T5-022, Revision 0. Westinghouse Electric Company LLC. August 2007. TRIM Ref. 2011/93789.

157 *Ergonomic requirements for office work with visual display terminals (VDTs). Part 3: Requirements for Office Work with Visual Display Terminals (VDTs).* BS EN ISO 29241-3. British Standards Institute, London. June 1993.

158 *AP1000 Secondary Dedicated Safety Panel Outline*. APP-JC01-V1-360 Revision B. Westinghouse Electric Company LLC. 2008. TRIM Ref. 2011/93660.

159 *Remote Shutdown Workstation Panel Outline*. APP-JC01-V1-150 Revision A. Westinghouse Electric Company LLC. September 2007. TRIM Ref. 2011/93652.

160 *Remote Shutdown Room Layout Top View*. APP-JC01-V1-100 Revision D. Westinghouse Electric Company LLC. February 2008. TRIM Ref. 2011/81460.

161 *Plant Lighting System Specification Document*. Westinghouse Electric Company LLC. APP-ELS-E8-001 Revision 0. November 2007. TRIM Ref. 2011/79430.

162 *Woodson W E, Tillman B and Tillman P, Human Factors Design Handbook*. New York: McGraw Hill. 1992.

163 *BS 5266-10:2008. Guide to the design and provision of emergency lighting to reduce the risks from hazards in the event of failure of the normal lighting supply.* British Standard Institution. 2008.

164 Not used

165 Framework for AP1000 Severe Accident Management Guidance. APP-GW-GJ-R-400 Revision A. Westinghouse Electric Company LLC. January 2007. TRIM Ref. 2011/473948, 2011/473958, 2011/473963

166 *NS-G-2.15. Severe Accident Management Programmes for Nuclear Power Plants Safety Guide*. IAEA Safety Standards Series (International Atomic Energy Agency). July 2009.

167 *BS EN ISO 9921:2003. Ergonomics. Assessment of speech communication*. British Standard Institution. November 2003.

168 *New Nuclear Power Stations. Generic Design Assessment. Strategy for Working with Overseas Regulators* – NGN04 . March 2009. TRIM Ref. 2009/271297.

169 *New Nuclear Power Stations. Generic Design Assessment. Safety assessment in an International Context* – NGN05. March 2009. TRIM Ref. 2009/271327.

170 *Nuclear Energy Agency – Multinational Design Evaluation Programme*. http://www.oecd-nea.org/mdep/.

171 *Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design (NUREG-1793). Chapter 18 – Human Factors Engineering*. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1793/chapter18.pdf.

172 Not used.

173 *New Nuclear Power Stations. Generic Design Assessment. Guidance on the Management of GDA Outcomes.* Version 1. HSE. June 2010. TRIM Ref. 2010/262572.

174 *AP1000 Squib Valve Failure Modes and Effects Analysis (FMEA).* APP-PV70-GRA-001 Revision 0. Westinghouse Electric Company LLC. March 2010. TRIM Ref. 2011/94136.

175 *IEEE Standard for Information Technology - Software Life Cycle Processes*. IEEE/EIA 12207.0. 1996.

176 *AP1000 Main Control Room Staff Roles and Responsibilities.* Revision 2. Westinghouse Electric Company LLC. June 2007. TRIM Ref. 2011/79758.

177 *Computer Based procedure Systems: Technical Basis and Human Factors Review Guidance*. NUREG/CR-6634. US Nuclear Regulatory Commission. March 2000.

178 *Step 4 Mechanical Enigineering Assessment of the Westinghouse AP1000.* ONR-GDA-AR-11-010 Revision 0. TRIM Ref. 2010/581521.

179 *Background and explanatory information. GDA Issue GI-AP1000-HF-01 Revision 0.* TRIM Ref. 2011/326260.

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
Work Stream 1	
UKP-GW-GL-042, Rev. 1	AP1000 Human Factors Program and Assessment for the United Kingdom
UKP-GW-GL-069, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case as reflecting the UK AP1000 PRA update
UKP-GW-GL-070, Rev. 0	United Kingdom AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA
UKP-GW-GL-071, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case as reflecting the UK AP1000 Low Power and Shutdown PRA
UKP-GW-GL-072, Rev. 0	United Kingdom AP1000 Supplemental Information for the Human Factors Safety Case – Potential Improvements as proposed in the ALARP Analysis
UKP-GW-GL-073, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Identified Non-Core Damage Human Errors with possible Radioactive Release
UKP-GW-GL-074, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability
UKP-GW-GL-075, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults
UKP-GW-GL-076, Rev. 0	United Kingdom AP1000 Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms
EPS-GW-GL-700, Rev, 0	AP1000 European Design Control Document
UKP-GW-GLR-003, Rev. 0	AP1000 Fault Schedule for the United Kingdom
UKP-GW-GL-022, Rev. 0	UK AP1000 Probabilistic Risk Assessment
APP-GW-GJP-204, Rev. 3	Emergency Operating Procedure E-3, Steam Generator Tube Rupture
UKP-GW-GL-732, Rev. 1	AP1000 Pre-construction Safety Report
UKP-GW-GL-710, Rev. 0	UK Compliance Document: Section A, UK Safety Case Overview
APP-GW-GER-005, Rev. 1	Safe and Simple: The Genesis of the AP1000 Design
APP-GW-GRR-009, Rev. 1	AP1000 Design Reliability Assurance Program
WCAP 14655	Designer's Input for the Training of Human Factors Engineering Verification and Validation Personnel
APP-GW-GJP-201, Rev. 3	Emergency Operating Procedure E-0, Reactor Trip or Safeguards Actuation
APP-GW-GJR-201, Rev. 1	Background Information for Emergency Operating Procedure E-0, Reactor Trip or Safeguards Actuation
APP-OCS-J1R-220, Rev. B	Operational Sequence Analysis (OSA-2)
APP-GW-GJP-202, Rev. 3	Emergency Operating Procedure E-1, Loss of Reactor or Secondary Coolant
APP-GW-GJP-202 Rev. 2	Emergency Operating Procedure, E-1 LOCA Outside Containment
APP-CVS-M3-001, Rev. 1	AP1000 Chemical and Volume Control System, System Specification Document
PRA-GSC-251	AP600 PRA, Internal Flooding Analysis
APP-GW-GJP-213, Rev. 0	Emergency Operating Procedure FR-H.1, Response to Loss of Heat Sink
APP-GW-GRP-001, Rev. 0	AP1000 Local Panels and Maintainability Human Factors Design Guidelines
APP-OCS-JCR-001, Rev. A	AP1000 Local Panels and Maintainability Human Factors Engineering Assessment

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
WCAP-14644-Nom Rev. 1	AP600/AP1000 Functional Requirements Analysis and Function Allocation
APP-PXS-M3-001, Rev. 2	Passive Core Cooling System, System Specification Document
APP-OCS-J1A-020, Rev. 0	UK AP1000 Function Based Task Analysis Data
APP-GW-GL-011, Rev. 0	AP1000 Identification of Critical Human Actions and Risk Important Tasks
APP-OCS-J1R-120, Rev. B	Operational Sequence Analysis (OSA-1)
APP-GW-GLR-040, Rev. 1	Plant Operations, Surveillance, and Maintenance Procedures.
APP-RNS-GJP-101, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 17, Normal Residual Heat Removal System
APP-GW-GJP-343, Rev. B	Abnormal Operating Procedure AOP 343, Loss of Normal Residual Heat Removal
APP-PXS-GJP-801 Rev. A	CMT Valve Surveillance and IST Testing
APP-PXS-GJP-101. Rev. D	Passive Cover Cooling System. Attachment 4: Filling and Venting the Core Makeup Tanks
APP-FHS-M3-001, Rev. 0	AP1000 Fuel Handling System, System Specification Document
APP-PMS-J1-001, Rev. 3	Protection and Safety Monitoring System Functional Requirements
APP-PMS-J4-002, Rev. A	AP1000 Protection and Safety Monitoring System Design Requirements
APP-PMS-J4-020, Rev. 0	System Design Specification for the Protection and Safety Monitoring System
APP-GW-GLR-146	AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report
APP-DAS-J7-001, Rev. B	AP1000 Diverse Actuation System - System Specification Document
APP-GW-GJP-3, Rev. B	AOP-336 Malfunction of PMS
APP-GW-GJP-250, Rev. 1	Emergency Operating Procedure F-0, Critical Safety Function Status Trees
APP-GW-GJR-223, Rev. 0	Emergency Operating Procedure, FR-S.1 Response to Nuclear Power Generation – ATWS
APP-DAS-GJP-101 Rev. C	APP-DAS-GJP-101 Rev. C. (2008) Diverse Actuation System
APP-JC01-V1-311 Rev. C	AP1000 Primary Dedicated Safety Panel Layout
APP-DAS-GEH-001, Rev. 1	AP1000 Diverse Actuation System Design Process
APP-JC01-V1-420. Rev. B	Diverse Actuation System Panel Layout
APP-GW-GJP-230 Rev. 1	Emergency Operating Procedure, SDF-0 Shutdown Critical Safety Function Status Tree
APP-GW-GJP-231 Rev. 2	Emergency Operating Procedure, SDF-1 Response To Loss Of RCS Inventory During Shutdown
Work Stream 2	
UKP-GW-GL022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 30, Human Reliability Analysis
UKP-GW-GL022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 43, Attachment 43C Evaluation of Operator Actions
APP-OCS-J1R-220, Rev. B	AP1000 Operational Sequence Analysis (OSA-2) Summary Report
UKP-GW-GL022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 43, Release Frequency Quantification
UKP-GW-GL022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 33 Fault Tree and Core Damage Quantification
UKP-GW-GL022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 54 Low-Power and Shutdown Risk Assessment
Work Stream 3	
APP-GW-GER-005	The Genesis and Process of the AP1000 Design APP

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
UKP-GW-GL-732, Rev. 1	AP1000 Pre-construction Safety Report
UKP-GW-GL-042, Rev. 2	AP1000 Human Factors Program and Assessment for the United Kingdom UKP
APP-OCS-GBH-001, Rev. 1	AP1000 Human Factors Engineering Program Plan
APP-OCS-JCR-001, Rev. A	AP1000 Local Panels and Maintainability Human Factors Engineering Assessment
APP-OCS-J1R-220, Rev. B	AP1000 Operational Sequence Analysis (OSA-2) Summary Report
UKP-GW-GL-076, Rev. 0	Supplemental Information for the UK AP1000 Human Factors Safety Case - Operator Error Mechanisms
WNA-WI-00039-WAPP, Rev. 1	RRAS Nu-Start/DOE Design Finalization Human Factors Engineering Design Issues Tracking System
APP-GW-GRP-001, Rev. 0	Local Panel and Maintainability Human Factors Design Guidelines
APP-OCS-J1-002	HSI Design Guidelines
APP-OCS-GEH-120, Rev. B	AP1000 Human Factors Engineering Design Verification Plan
WCAP-16555, APP-GW-GL-011, Rev. 0	AP1000 Identification of Critical Human Actions and Risk Important Tasks
WCAP-14645	Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant
APP-GW-GLR-001, Rev. 3	Operational Assessment for AP1000
V3P2-AP1000, Rev. A	European Utility Requirements (EUR), Volume 3 AP1000 Subset, Chapter 2 Highlights of the Compliance Analysis
VSP/VSG0223	Operating Experience Identified at the Consortium Corrective Action Interface Meeting
VSP/VSG0475	Operating Experience Identified at the Consortium Corrective Action Interface Meeting
APP-GW-GEE-1765, Rev A	RNS Pump Room (A/B) Overhead Monorails
APP-GW-GEE-1630, Rev A	Add Hatch and Padeyes to RNS Valve Room for Maintenance
APP-GW-G1R-007, Rev. A	Operating Experience to Apply to Advanced Light Water Reactor Designs March
APP-MB01-GRR-001, Rev. 0	AP1000 Steam Generator Operating Experience Report
APP-ME30-VDR-001, Rev. 0	Use of Plate Heat Exchangers in Westinghouse AP1000 - Summary Report
APP-GW-GLR-001 Rev. 3	Operational Assessment for AP1000
APP-CVS-G1-002, Rev. A	Chemical and Volume Control System Institute of Nuclear Power Operations Operating Experience
DCP-PAR004	Meeting Minutes of AP1000 Polar Crane - Load Bearing Components, Intermediate Design Review 01/08/11
APP-PV70-GER, Rev. B	Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary
APP-GW-GEE-190	Rev. 0, Main Control Room Layout
App-GW-GEE-490, Rev. 2	AP1000 Auxiliary Building Fuel Handling Area Modifications
FOKWMS0410	Use of Squib Valves in IRWST Lines
FOK/WMS0383	Squib valve review package
APP-PXS-M3C-038, Rev. 3	Squib Valve Functional Requirements for Reactor Coolant System (RCS) Automatic Depressurization System Stage 4 (ADS-4) Valves
APP-PXS-M3C-039, Rev. 1	Squib Valve Functional Requirements for PXS IRWST Injection Isolation and Containment Recirculation Isolation Squib Valves

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
N/A	ADS SQUIB ROOMS 11301 and 11302 MAINTAINABILITY STUDY - Situation Overview Paper
APP-PXS-GJP-804	IRSWT inject and CTMT Recirc Valve Booster Assembly Replacement and Testing
N/A	Westinghouse Level II Policies and Procedures
WCAP-16096-NP-A Rev. 1A	Software Program Manual for Common Q Systems
EPS-GW-GL-700	AP1000 European 18. Human Factors Engineering Design Control Document
APP-GW-GAP-420	Westinghouse Level II Operating Procedures
APP-GW-G1-011, Rev. 1	Standard Plant Metrication
EPS-GW-GL-700, Rev. 1	Design Control Document
Work Stream 4	
UKP-GW-GL-042, Rev. 1	AP1000 Human Factors Program and Assessment for the United Kingdom (Safety Case)
UKP-GW-GL-740, Rev. 0	AP1000 Safety Case Overview – Roadmap
EPS-GW-GL-700, Rev. 1	AP1000 European Design Control Document. Chapter 18 Human Factors
APP-GW-GER-005, Rev. 1	Safe and Simple: The Genesis and Process of the AP1000 Design
N/A	AP1000: Safe, Simple, Innovative, Westinghouse Electric Company LLC Information Brochure, 2007
UK-GW-GL-022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 30
UKP-GW-GLR-003, Rev. 0	AP1000 Fault Schedule for the United Kingdom
APP-GW-GRR-009, Rev. 1	AP1000 Design Reliability Assurance Program
N/A	Westinghouse slides on competence management presented to inspection visit, 15/09/2010
WCAP-14655, Rev. 1	Designer's Input for the Training of the Human Factors Engineering Verification and Validation Personnel
APP-GW-GRJ-011	Review of Operating Experience and the Application of the Design of the AP600
APP-OCS-GJR-001 (WCAP-14645-NP)	Human Factors Engineering Operating Experience Review Report for the AP1000 Nuclear Power Plant, Revision 3
APP-GW-G1R-007	Operating Experience to Apply to Advanced Light Water Reactor Designs
APP-OCS-GBH-001, Rev. 1	AP1000 Human Factors Engineering Program Plan
WNA-PN-00057-WAPP, Rev. 1	NuStart/DOE Design Finalization Operations and Control Center Systems Project Plan
03/31/10 E6_WEC	Westinghouse Level II Policies and Procedures
APP-GW-GEP-010, Rev. 2	Process and Procedure for AP1000 Internal Open Items
Westinghouse Procedure NSNP 3.4.1, Rev. 2	Change Control for the AP1000 Program
WCAP-15847	AP1000 Quality Assurance Procedures Supporting NRC Review of AP1000 DCD Sections 18.2 and 18.8, Revision 1, December 2002.
WNA-PN-00043-WAPP Rev. 1	NuStart/DOE Design Finalization Program Project Plan
APP-GW-GJP-250, Rev. 1	Critical Safety Function Status Trees
WCAP-13793	The AP600 System/Event Matrix, June 1994.
APP-GW-GLR-003, Rev. 1	AP1000 Adverse System Interactions Evaluation Report
WCAP-14694	Designer's Input to Determination of the AP600 Main Control Room Staffing Level

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-GW-GLR-082	Execution and Documentation of the Human System Interface Design Implementation Plan. May 2007
APP-CVS-M3-001, Rev. 1	Chemical and Volume Control System System Specification Document
WCAP-14651	Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan, Revision 2, May 1997
APP-GW-GLR-011	Execution and documentation of the human reliability analysis/Human Factors engineering integration
WCAP-16555 APP-GW-GL-011, Rev. 0	AP1000 Identification of Critical Human Actions and Risk Important Tasks
APP-OCS-GJR-002, Rev. B	Concept of Operation
APP-OCS-GGR-110-P, Rev. 1	AP1000 Technical Support Center and Emergency Operations Facility Workshop
APP-OCS-GGR-105, Rev. 0	Report on the AP1000 Main Control Area Layout Workshop
WCAP-14694	Designer's Input to Determination of the AP600 Main Control Room Staffing Level (1996)
EPS-GW-GL-700, Rev. 1	European DCD, Chapter 13 Conduct of operation.
APP-GW-GLR-010, Rev. 2	AP1000 Main Control Room Staff Roles and Responsibilities
APP-OCS-GGR-110	AP1000 Technical Support Center and Emergency Operations Facility Workshop
APP-OCS-J0A-001	AP1000 Human Factors Engineering Analysis to Support Technical Support Center and Emergency Operations Facility Design
APP-GW-GJRSO6 Rev. B	Background Information for AOP-306, Evacuation Of Control Room
APP-OCS-J1R-100, Rev. 0	A Function-Based Task Analysis Methodology and Implementation for AP1000
APP-OCS-J1A-030, Rev. 0	AP1000 Function-Based Task Analysis Summary Report
WCAP-14644, Rev. 1	AP600/AP1000 Functional Requirements Analysis and Function Allocation
APP-OCS-J1R-110, Rev. 0	Operational Sequence Analysis Methodology
APP-OCS-J1R-120, Rev. 0	AP1000 Operational Sequence Analysis (OSA-1) Summary Report
APP-OCS-J1R-210, Rev. 1	AP1000 Operational Sequence Analysis 2 (OSA 2) Implementation Plan
APP-OCS-J1R-220, Rev. B	AP1000 Operational Sequence Analysis (OSA 2) Summary Report
WCAP-14695	Description of the Westinghouse Operator Decision Making Model and Function Based Task Analysis Methodology
APP-GJ01-GTP-001, Rev. A	AP1000 Job and Task Analysis Procedure
APP-GJ01-GTP-002, Rev. B	Training Material Design and Development Procedure
APP-OCS-GER-041	AP1000 The Incorporation of Human Factors Engineering into the Development of the AP1000 Plant Training Programs
APP-DWS-M3-001, Rev. D	RD Radiologically controlled area ventilation system – System Specification Document
APP-ELS-E8-001, Rev. 0	Plant Lighting System – System Specification Document
APP-OCS-J7-001, Rev. B	AP1000 Operations and Control Centers System, System Specification Document
APP-OCS-J1-009, Rev. B	Operations and Control Centers System Functional Requirements
APP-GW-P1-002, Rev. 0	AP1000 General Layout Criteria
WEC00326N	Response Regulatory Observation RO-AP-1000-086 and Regulatory Observation Actions RO-AP1000-086A1 and A2 – Health Physics and Radioactive Waste Facilities

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
WCAP-16096-NP-A, Rev. 1A	Software Program manual for Common Q Systems
APP-OCS-JCR-001 AP1000, Rev. A	Local Panels and Maintainability Human Factors Engineering Assessment
EPS-GW-GER-012, Rev. A	AP1000 Decommissioning Summary Report
N/A	Decommission of AP1000, Presentation to EA / ND, Pittsburgh, 25 February 2010
APP-OCS-J1-002, Rev. 1	AP1000 Human System Interface Design Guidelines
APP-GW-GRP-001, Rev. 0	AP1000 Local Panels and Maintainability Human Factors Design Guidelines
WCAP-16801-P, APP-GW-GLR-082	Execution and Documentation of the Human System Interface Design Implementation Plan
APP-OCS-J4V-001 AP1000, Rev. A	Operation Control Centers Alarm Presentation System Design Specification
APP-OCS-J1-001, Rev. 0	AP1000 Alarm Presentation System Functional Requirements
WNA-DS-01045-GEN, Rev. 1	Standard Alarm Presentation System Functional Requirements
APP-OCS-Z0-001	Alarm Presentation System Design Specification
APP-OCS-J1-007, Rev. 0	AP1000 Wall Panel Information System Functional Requirements
APP-GW-GJP-336, Rev. B	Malfunction of PMS
APP-DAS-GJP-101, Rev. C	Diverse Actuation System
APP-GW-J1-010, Rev.1	AP1000 Instrumentation and Control System Requirements Documentation
APP-GW-54-001, Rev.1	AP1000 I&C System Design Specification
APP-OCS-J1-010 AP1000, Rev. 0	Display System Functional Requirements
APP-DDS-J4V-002, Rev. D	Specification of Static and Dynamic Elements for Display
APP-DDS-J4V-001, Rev. C	Display Design Specification
APP-OCS-J1-020, Rev. 1	AP1000 Computerized Procedures System Functional Requirements
APP-FHS-M3-001, Rev. 0	AP1000 Fuel Handling System - System Specification Document.
APP-GW-GZP-002 Rev. 0	AP1000 Component Tagging and Labelling Procedure
WCAP-14690, Rev. 1	Designer's Input to Procedure Development for the AP600
APP-OCS-GER-031, Rev. A	AP1000 The Incorporation of Human Factors Engineering into the Development of AP1000 Plant Procedures
APP-GW-GLR-040, Rev. 1	Plant Operations, Surveillance, and Maintenance Procedures
APP-GW-GJR-321 Rev. B	Background Information For Abnormal Operating Procedure MALFUNCTION OF DDS
APP-OCS-GGR-100, Rev. 0	AP1000 Human Factors Multidiscipline Preliminary Design Review Report
APP-OCS-GGR-101, Rev. 0	AP1000 Human Factors Engineering Design Review #2 Report
APP-PMS-GGR-021	PMS Functional Design Intermediate Design Review Report.
APP-CVS-GGR-201	RA CVS Preliminary Design Review Report.
APP-PSS-GGR-201	RA Primary Sampling System Intermediate Design Review Report.
APP-PSS-GGR-200	RA Primary Sampling System Intermediate Design Review Package
APP-FWS-GGR-001	Feedwater System Preliminary / Intermediate Design Review Report.

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-MT02-GGR-301	Accumulator Tank Final Design Review Report.
DCPPAR0004	Meeting Minutes of AP1000 Polar Crane - Load Bearing Components, Intermediate Design Review.
WCAP-10170	Emergency Response Facilities Design and V&V Process, April 1982
WCAP-15860, Rev. 2	Programmatic Level Description of the AP1000 Human Factors Engineering Verification and Validation Plan
APP-OCS-T5-020	Engineering Test Plan for AP1000 Soft Controls
APP-OCS-T5-022	Phase 2 Engineering Test Plan for AP1000 Control Room Integration
APP-OCS-T2R-020, Rev. 0	AP1000 Engineering Tests Phase 1 Test Report
APP-OCS-T2R-022, Rev. 0	AP1000 Engineering Tests Phase 2 Test Report
APP-OCS-T2R-030, Rev. 0	AP1000 Human Factors Engineering Test Phase 3 Test Report
APP-OCS-GEH-320, Rev. D	AP1000 Human Factors Engineering Integrated System Validation Plan
WCAP-14396, Rev. 3	Man-in-the-Loop Test Plan Description
WNA-WI-00039-WAPP, Rev. 1	Human Factors Engineering Design Issues Tracking System"
APP-PMS-J4-001, Rev. 0	AP1000 Post-Accident Monitoring System Functional Specification
APP-GW-GJP-201, Rev. 3	Reactor Trip or Safeguards Actuation
APP-GW-GJP-202, Rev. 3	Loss of Reactor or Secondary Coolant
APP-GW-GLR-001, Rev. 3	Operational Assessment for AP1000
UKP-GW-GL-045, Rev. 0	AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards
APP-GW-VW-002, Rev. 0	AP1000 Design for Inspectability Program: ISI Requirements for Class 2 and 3 Components and Core Internals Structures
Simulator videos provided by WEC	TQ-AP1000-560 Full Response AP1000 Simulator Video Part 1: Main Control Room Overview TQ-AP1000-560 Full Response AP1000 Simulator Video Part 2: Alarm System TQ-AP1000-560 Full Response AP1000 Simulator Video Part 3: Demonstration of Steam Generator Tube Rupture TQ-AP1000-560 Full Response AP1000 Simulator Video Part 4: Computerised Procedure System
Work Stream 5	
UKP-GW-GL-732, Rev. 1	AP1000 Pre-construction Safety Report
EPS-GW-GL-700, Rev. 1	AP1000 European Design Control Document
WCAP 14651, Rev. 2	Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan
APP-OCS-J1A-030, Rev. 0	Function-Based Task Analysis Summary Report
APP-OCS-J1R-120, Rev. 0	AP1000 Operational Sequence Analysis (OSA-1) Summary Report
APP-OCS-J1R-220, Rev. B	AP1000 Operational Sequence Analysis (OSA-2) Summary Report
APP-OCS-T2R-020, Rev. 0	AP1000 Engineering Tests Phase 1 Test Report
APP-OCS-T2R-022, Rev. 0	Phase 2 Test Report
APP-OCS-T2R-030, Rev. 0	AP1000 Human Factors Engineering Test Phase 3 Report
WCAP-14644-NP, Rev. 1	AP600/AP1000 Functional Requirements Analysis and Function Allocation
APP-OCS-J1R-100, Rev. 0	Function-Based Task Analysis Methodology and Implementation for AP1000

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-OCS-J1A-020, Rev. 0	Function-Based Task Analysis Data
APP-OCS-J1R-110, Rev. 0	Operational Sequence Analysis Methodology
APP-GW-GL-011, Rev. 0	AP1000 Identification of Critical Human Actions and Risk Important Tasks
WCAP-14695, Rev. 0	Description of the Operator Decision Making Model and Function-Based Task Analysis Methodology
UKP-GW-GL-022, Rev. 0	UK AP1000 Probabilistic Risk Assessment, Chapter 30, Human Reliability Assessment
APP-OCS-J1R-210, Rev. 1	AP1000 Operational Sequence Analysis (OSA-2) Implementation Plan
WCAP-14396, Rev. 3	Man-in-the-Loop Test Plan Description
APP-OCS-T5-020, Rev. 0	AP1000 Engineering Test Plan for Soft Controls
UKP-GW-GL-732, Rev. 2	AP1000 Pre-construction Safety Report
APP-OCS-T5-022, Rev.0	Phase 2 Engineering Test Plan for AP1000 Control Room Integration
UKP-GW-GL-042, Rev. 1	AP1000 Human Factors Program and Assessment for the United Kingdom
APP-OCS-J1-002, Rev. 1	AP1000 Human System Interface Design Guidelines.
WNA-CN-00118-GENm, Rev. 0	China, United Kingdom and United States Adult Population Anthropometric Data
APP-JC01-Z0-001, Rev. B	Design Specification for Control Room Consoles and Panels
APP-JC01-V1-001, Rev. E	Main Control Area Layout Top View
APP OCS GGR 105	Report on AP1000 Main Control Area Workshop
APP-JC01-V1-200, Rev. B	Senior Reactor Operator Console Outline
APP-JC01-V1-250, Rev. B	Reactor Operator Console (A) Outline
APP-JC01-V1-300, Rev. C	Primary Dedicated Safety Panel Outline
APP-JC01-V1-360, Rev. B	Secondary Dedicated Safety Panel Outline
APP-JC01-V1-400, Rev. B	Diverse Actuation System Panel Outline
APP-JC01-V1-420, Rev. B	Diverse Actuation System Panel Layout
APP-JC01-V1-101, Rev. A	Remote Shutdown Room Layout Side View
APP-JC01-V1-150, Rev. A	Remote Shutdown Workstation Panel Outline
APP-JC01-V1-100, Rev. D	Remote Shutdown Room Layout Top View.
APP-GW-GRP-001, Rev. 0	AP1000 Local Panels and Maintainability Human Factors Guidelines
EUR Vol. 3F, Chapter 2	European Utility Requirements for LWR Nuclear Power Plants. Chapter 2, Highlights of the Compliance Analysis
APP-ELS-E8-001, Rev. 0	Plant Lighting System Specification Document
APP-VES-M3-001, Rev. 0	Main Control Room Emergency Habitability System, System Specification Document
APP-VAS-M3-001, Rev. D	Radiologically Controlled Area Ventilation System Specification Document
APP-12401-GER-001, Rev. 0	Evaluation of the Noise in the AP1000 Main Control Room
APP-GW-J4-001, Rev. 1	AP1000 I&C System Design Specification
APP-GW-J1-010, Rev. 1	AP1000 I&C System Requirements Specification
APP-DDS-J4V-002, Rev. E	AP1000 Specification of Static and Dynamic Elements for Display

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-PMS-GHY-009, Rev. A	AP1000 Protection and Safety Monitoring System Software Design Description for the Safety Display
APP-OCS-GJR-002, Rev. B	Concept of Operation
APP-PMS-J4-002, Rev. A	AP1000 Protection and Safety Monitoring System Design Requirements
CCD/1049/REP/002/10, Ver. 3	UK Nuclear Worker Stereotypical Representation relative to Westinghouse AP1000 Nuclear Plant Human Factors Design. Combined Phase 1 and 2 Report. CCD Report
WNA-CT-00146-GEN, Rev. 2	Standard Windows Ovation Health Display Generation Tool (HDGT)
APP-DDS-J4V-001, Rev. C	AP1000 Display Design Specification
APP-OCS-J4-002, Rev. A	AP1000 Wall Panel Information System Hardware Design Specification
APP-OCS-J1-007, Rev. 2	AP1000 Wall Panel Information System Functional Requirements
APP-PMS-J1-001, Rev. 0	AP1000 Protection and Safety Monitoring System Functional Requirements
APP-JC01-V1-311, Rev. C	AP1000 Primary Dedicated Safety Panel Layout. Drawing
APP-JC01-V1-370, Rev. C	AP1000 Secondary Dedicated Safety Panel Layout. Drawing
APP-JC01-V1-120, Rev. C	Remote Shutdown Workstation Panel Layout
APP-G1-GMP-007, Rev. 0	Equipment Identification Labels
APP-G1-GMP-004, Rev. 0	Conventional Colors for Equipment and Piping.
APP-GW-GZP-002, Rev. 0	AP1000 Component Tagging and Labelling Procedure
APP-OCS-JCR-001, Rev, A	Local Panels and Maintainability Human Factors Engineering Assessment
APP-OCS-J1-001, Rev. 0	Alarm Presentation System Functional Requirements
WNA-DS-01045- GEN, Rev. 1	Standard Alarm Presentation System Functional Requirements
APP-OCS-J4V-001, Rev. A	AP1000 Operation Control Centers Alarm Presentation System Design Specification
WCAP-14690, Rev. 1	Designer's Input to Procedure Development for the AP600
APP-OCS-GER-031, Rev. A	AP1000 The Incorporation of Human Factors Engineering into the Development of the AP1000 Plant Procedures
APP-DDS-J4-120, Rev. 0	Computerized Procedures Software Requirements Specification
APP-OCS-J1-020, Rev. 1	Computerized Procedures System Functional Requirements
WNA-DS-01619-GEN, Rev. 0	Standard Computerized Procedures Software Requirements Specification.
APP-GW-GJP-200, Rev. G	Writer's Guideline for Two Column Procedures
APP-GW-GJP-201, Rev. 3	Emergency Operating Procedure. E-0. Reactor Trip or Safeguards Actuation
APP-GW-GJP-204, Rev. 3	Emergency Operating Procedure. E-3. Steam Generator Tube Rupture
APP-GW-GJP-304, Rev. 3	Abnormal Operating Procedure. AOP-304. Steam Generator Tube Leak
APP-GW-GJP-250, Rev. 1	Emergency Operating Procedure. F-0. Critical Safety Function Status Trees
APP-GW-GJP-230, Rev. 1	Emergency Operating Procedure. SDF-0. Shutdown Critical Safety Function Status Tree
APP-GW-GJP-210, Rev. 2	Emergency Operating Procedure. FR-C.1. Response to Inadequate Core Cooling
APP-PCS-GJP-401, Rev. A	Alarm Response Procedure – Passive Containment Cooling System
APP-RCS-GJP-401, Rev. A	Alarm Response Procedure – Reactor Coolant System
APP-GW-GJP-107, Rev. D	General Operating Procedure.GOP-107.Plant Heatup from Mode 4 to Normal Operating Temperature

Table 22

Generic Design Assessment Supporting Documentation for Human Factors Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-GW-GJP-108, Rev. C	General Operating Procedure.GOP-108.Plant Startup from Normal Operating Temperature to Less than 5% Power
APP-GW-GJP-100, Rev. G	AP1000 Normal Operating Procedures (NOP) Writer's Guideline
APP-GW-GJP-800, Rev. A	AP1000 Maintenance, Test, Inspection and Surveillance (MTIS) Writer's Guideline
APP-GW-GLR-040, Rev. 1	Plant Operations, Surveillance, and Maintenance Procedures
APP-GW-GLR-010, Rev. 2	AP1000 Main Control Room Staff Roles and Responsibilities
WCAP-14694	Designer's Input to Determination of the AP600 Main Control Room Staffing Level
APP-GW-GER-005, Rev. 1	Safe and Simple: The Genesis of the AP1000 Design

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-01	The licensee shall provide additional evidence / re-substantiation of the human actions claimed within the AP1000 UK HF safety case with particular consideration of ND's qualitative assessment of 41 human actions. In addition the licensee shall consider the ND quantification of 13 human actions as part of the HRA update. This should include consideration of those assumptions ONR considers not to be currently substantiated.	4.2.1.1	Prior to Fuel Load
AF-AP1000-HF-02	The licensee shall consolidate the qualitative HF analysis presented for the UK HF safety case and apply it to the revision of the PSA.	4.2.1.1	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-03	The licensee shall re-quantify the HEPs in the HRA recognising my comments in this GDA assessment report relating to over optimism. Alternatively additional qualitative evidence may be presented to support the extant numerical claims.	4.2.1.1	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-04	The licensee shall develop the operating philosophy and procedural and training support relating to severe accident management. This should specifically focus on the transition from design basis accidents to beyond design basis accidents. I expect the licensee's approaches in this area to conform to recognised good practice as defined by the IAEA.	4.2.1.2	Prior to Fuel Load
AF-AP1000-HF-05	When revising the HRA, the licensee shall consider the human reliability data relating to omission errors when following computerised procedures. I suggest that the most relevant THERP data for such tasks are items 3 and 4 of Table 20-7 if used with the full Error Factor weighting and uncertainty bounds	4.2.1.3	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-06	The licensee shall assess the quality of checklists available (for those plant procedures that are paper based in terms of their support to human reliability; and consider the use of items 1 and 2 of THERP Table 20-7 to model errors of omission.	4.2.1.3, 4.6.7	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-07	The licensee shall reassess the human reliability data relating to checking as a recovery mechanism. I consider items 1 or 2 from THERP table 20-22 more appropriate for modelling recovery from operator errors and I suggest that this data be applied as part of the HRA revision.	4.2.1.3, 4.3.3.1, 4.3.4.1	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-08	The licensee shall reassess quantitative human error dependency as part of the revision to the HRA. The human error dependency assessment should be fully supported by qualitative HF assessment, which highlights the design features to mitigate dependence mechanisms.	4.2.1.3, 4.3.3.3, 4.3.4.1, 4.3.4.2, 4.3.4.3, 4.3.4.4	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-09	The licensee shall ensure that the revision to the HRA models the actual post fault operating regime to be applied. This shall include an accurate representation of the staffing structure and explicitly model any dependency that results from this.	4.2.1.3, 4.3.3.1, 4.3.4.4	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-10	The licensee shall include the additional HEPs identified as part of the UK HF safety case into fault sequences as part of the PSA update.	4.2.2	Prior to Fuel Load (in line with PSA assessment finding / expectation for the revision to the PSA)
AF-AP1000-HF-11	The licensee shall develop, maintain and substantiate the HF assumptions as the safety case develops.	4.2.2	Prior to first structural concrete

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-12	The licensee shall review the Westinghouse ALARP case for HF to develop, amplify and complete the ALARP case as part of the site specific PCSR. This development should specifically consider the optioneering of and requirements for manual/operator actions.	4.2.3	Prior to Nuclear island safety related concrete
AF-AP1000-HF-13	The licensee shall reassess the Type A human error quantifications in light of decisions relating to maintenance regimes and frequencies and revise as appropriate.	4.3.1	Prior to Fuel Load
AF-AP1000-HF-14	The licensee shall consider the applicability of extant HRA methods to the AP1000 HRA revision; and note my regulatory expectations in this regard as cited in SAP EHF. 10 and TAG 063 on HRA. In the absence of justified and directly applicable HRA data, the licensee should apply a precautionary principle to assigning HEPs (e.g. the use of uncertainty bounds).	4.3.2	Prior to Fuel Load
AF-AP1000-HF-15	The licensee shall provide detailed justification of the appropriateness of sole reliance on alarms during the activation phase.	4.3.3.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-16	The licensee shall ensure that the revision to the HRA fully considers relevant plant interactions and models them appropriately.	4.3.3.1	Prior to Fuel Load
AF-AP1000-HF-17	The licensee shall develop management control procedures to ensure the availability of the STA or equivalent in the control room following an abnormal event.	4.3.3.1	Prior to Fuel Load
AF-AP1000-HF-18	The licensee shall reassess the slack time that Westinghouse claim to be available and its role in human error recovery and develop additional qualitative substantiation.	4.3.3.1	Prior to Fuel Load

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-19	The licensee shall model cognitive activation behaviour in the HRA revision.	4.3.3.2	Prior to Fuel Load
AF-AP1000-HF-20	The licensee shall reconsider and justify the screening value relating to the human action of failure to perform manual ADS operation following earlier automatic or manual activation failure during the later phases of an SGTR. In particular the potential for dependency should be considered and a qualitative HF assessment will be required.	4.3.3.3	Prior to Fuel Load
AF-AP1000-HF-21	The licensee shall model in the revised HRA the requirement for operators to recognise and diagnose that a scenario has moved into severe accident territory. This should be supported by a qualitative HF substantiation.	4.3.3.3	Prior to Fuel Load
AF-AP1000-HF-22	The licensee shall justify the stress modifiers applied to recovery situations as part of the update to the HRA.	4.3.4.2	Prior to Fuel Load
AF-AP1000-HF-23	The licensee shall provide additional qualitative evidence relating to dependency factors associated with human failure event LPM-REC01.	4.3.4.2	Prior to Fuel Load
AF-AP1000-HF-24	The licensee shall reassess the level of dependency assigned between actions ADN-MAN01 and CMN-MAN01 as part of the HRA update.	4.3.4.2	Prior to Fuel Load
AF-AP1000-HF-25	The licensee shall provide additional qualitative evidence relating to dependency factors associated with HFEs ADF-MAN01 and CVN-MAN0.	4.3.4.2	Prior to Fuel Load
AF-AP1000-HF-26	The licensee shall reassess the dependency level assigned to HFE PCN-MAN01 as part of the HRA update.	4.3.4.2	Prior to Fuel Load
AF-AP1000-HF-27	The licensee shall reassess the modelling associated with HFE CIB-MAN01 as part of the HRA update.	4.3.4.2	Prior to Fuel Load

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-28	The licensee shall reconsider the requirements for manual maintenance, and demonstrate that appropriate consideration has been given to alternative options including the feasibility of automation; in line with SAP EKP.5 and our ALARP requirements.	4.4.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-29	The licensee shall review the Westinghouse work on UK national population stereotypes; provide an impact assessment on the generic design of HMIs and justify how the UK AP1000 final interface designs comply with national population stereotypes. This should also form part of the V&V programme.	4.4.1, 4.6.5	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-30	The licensee shall specifically include maintenance and maintainability issues in their Human Factors V&V programme.	4.4.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-31	The licensee shall develop and submit a HFIP for UK AP1000 construction.	4.5, 4.5.3	Prior to first structural concrete
AF-AP1000-HF-32	The licensee shall provide a justification of the minimum staffing levels proposed.	4.5.1.2, 4.6.7	Prior to Fuel Load
AF-AP1000-HF-33	The licensee shall undertake, or justify otherwise, additional task analysis relating to non ‘core’ areas on a proportionate basis.	4.5.1.2	Prior to Fuel Load
AF-AP1000-HF-34	The licensee shall review the anthropometric data source applied to physical design of the AP1000 on a proportionate basis, against recognised UK data sets. This should recognise reasonable estimates of the secular trend of the intended operating lifetime of the plant.	4.5.1.2, 4.6.3.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-35	The licensee shall include the measurement of the usability of local to plant interfaces as part of their V&V programme.	4.5.1.2	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-36	The licensee shall provide a benchmark against current recognised good practice for the design of the baseline CPS system.	4.5.1.2	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-37	The licensee shall include HF requirements and good practice in the design of technical manuals.	4.5.1.2	Prior to Fuel Load
AF-AP1000-HF-38	The licensee shall include in their HFIP the requirement to develop an administrative control system.	4.5.1.2	Prior to first structural concrete
AF-AP1000-HF-39	The licensee shall identify and justify administrative controls that are required to maintain operations within the Safe Operating Envelope, at site specific PCSR stage.	4.5.1.2	Prior to first structural concrete
AF-AP1000-HF-40	The licensee shall review the HF contribution to the design for decommissioning.	4.5.1.2	Prior to Fuel Load
AF-AP1000-HF-41	The licensee shall justify or redevelop the scope of the Westinghouse proposals for V&V and ISV.	4.5.1.2	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-42	The licensee shall specifically include in the UK V&V and ISV, testing of the MCR staffing proposals and validation of the task completion times offered by Westinghouse in OSA-2.	4.5.1.2	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-43	The licensee shall provide estimates of maintenance times linked to the PSA system unavailability goals.	4.5.2	Prior to Fuel Load
AF-AP1000-HF-44	The licensee shall provide formal arrangements for HFI with other technical disciplines as part of their HFIP for UK construction of and AP1000.	4.5.2	Prior to first structural concrete

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-45	The licensee shall apply relevant good practice and modern HF standards and guidance to the continuing design and development of the UK AP1000 and its safety submissions fully reflecting the work required in response to the GDA Step 4 Assessment Findings. The standards and guidance applied should be justified as part of the continuing safety submissions.	4.5.5.1	Prior to first structural concrete.
AF-AP1000-HF-46	The licensee shall review and provide further analysis relating to the scenarios of the Westinghouse Operational Sequence Analysis 1.	4.6.2.2	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-47	The licensee shall undertake workload analysis using recognised analytical techniques.	4.6.2.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-48	The licensee shall review and reanalyse the Westinghouse operational sequence analyses 1 and 2 against their proposals for a UK staffing structure, should that differ from the Westinghouse proposals.	4.6.2.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-49	The licensee shall review, reconsider and supplement the task analyses for MTIS tasks on a proportionate and targeted basis.	4.6.2.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-50	The licensee shall specifically include the legibility (text sizes and saturated colour contrasts) of displays at the expected viewing angles and distances in the V&V programme, prior to final decisions being taken on screen angles and character/symbol sizes.	4.6.3.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-51	The licensee shall consider whether access panels on the RSWP should be ‘lift off’, and ensure that local maintenance lighting is provided.	4.6.3.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-52	The licensee shall consider the adequacy of access routes for the safe and timely evacuation of personnel in an emergency and the general accessibility of control rooms, panels and equipment in emergency situations.	4.6.3.4	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-53	The licensee shall review maintenance access dimensions; recognising the likely equipment (access) requirements.	4.6.3.4	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-54	The licensee shall provide additional justification that the lighting design of the MCR meets relevant standards and guidance.	4.6.4.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-55	The licensee shall develop appropriate controls as part of the work design for the spent fuel pond area, recognising the expected thermal environment in the area.	4.6.4.2	Prior to Fuel Load
AF-AP1000-HF-56	The licensee shall provide information on and justification for the expected humidity in the MCR and fuel handling areas.	4.6.4.2	Prior to Fuel Load
AF-AP1000-HF-57	The licensee shall reanalyse the noise and acoustic design of the MCR and provide additional HF justification	4.6.4.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-58	The licensee shall ensure the audibility of general emergency alarms throughout the plant during V&V.	4.6.4.3	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-59	The licensee shall reconfigure the labelling hierarchy on the DCIS screen displays proposed by Westinghouse against recognised good practice in this area.	4.6.5	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-60	The licensee shall reconsider and justify the terminology that is adopted to label the vertical scales on flow controller pop-ups on the DCIS.	4.6.5	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-61	The licensee shall redesign the PDSP and SDSP to remove the transposing of 'IRWST INJECTION' and 'IRWST RECIRCULATION' controls or justify the existing design.	4.6.5	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-62	The licensee shall ensure the consistency of information content and presentation between equivalent PMS and DCIS formats.	4.6.5	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-63	The licensee shall reconfigure the Westinghouse proposed layout of the RSWP controls in relation to the equivalent layout in the MCR on the PDSP and SDSP.	4.6.5	Prior to Fuel Load
AF-AP1000-HF-64	The licensee shall ensure that the use of manually operated valve controls does not exceed the maximum permissible operating forces that should be used, and that the separations between valve controls do not hinder their use.	4.6.5	Prior to Fuel Load
AF-AP1000-HF-65	The licensee shall justify the alarm philosophy and design proposed by Westinghouse in the UK context. The alarm presentation system shall be specifically investigated and focussed on as part of the V&V programme.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-66	The licensee shall justify that the specification of the alarm system provides an alarm for all safety related parameters / systems that require an operator response.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-67	The licensee shall clearly define the rules on alarm ownership, recognising the defined MCR staffing structure.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-68	The licensee shall remove the 'return to normal' chime within the APS, as it draws the attention of the operator to the alarms interface when there is no action necessary.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-69	The licensee shall undertake experiments to demonstrate that the global silencing of all alarms will not significantly affect human reliability. This warrants specific attention and a more concentrated focus above that of a V&V programme.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-70	The licensee shall reassess and justify the audible alarm levels proposed by Westinghouse. I consider the current proposals to be excessive and likely to cause disruption. This should be specifically investigated during V&V and set prior to commissioning.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-71	The licensee shall specifically include the clarity of colours and the ability to distinguish between them on workstation screens in the ambient lighting conditions as part of the V&V programme.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-72	The licensee shall demonstrate that the codes and abbreviations proposed for the primary and secondary system group alarm tiles are readily understood and are of practical use to the operators.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-73	The licensee shall consider the benefit of differing flash rates for different alarm priorities, to supplement the current coding of alarm prioritisation.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-74	The licensee shall review the contrast between the text and background in alarm lists to ensure legibility. This should specifically be included in the V&V.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-75	The licensee shall reconfigure the alarm list behaviours; recognising standard UK practice where an unhandled alarm line should flash.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-76	The licensee shall substantiate how operators will confirm their awareness of suppressed alarms particularly during shift handovers.	4.6.5.1	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-77	The licensee shall consider presenting the main tasks or task subsets on CPS displayed procedures hierarchically, to help the operators to divide the overall task into manageable perceptual chunks, whilst also focusing in more detail on their immediate tasks; or justify the existing design.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-78	The licensee shall provide justification of the means by which operators are alerted by the Parallel Information facility.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-79	The licensee shall ensure that the CPS incorporates design features that prevent operators from bypassing safety significant procedural steps, or justify the existing design.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-80	The licensee shall reconsider and justify the checking regime on the CPS displays.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-81	The licensee shall demonstrate the feasibility of switching between computer and paper based procedures (in the event of failure of the CPS).	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-82	The licensee shall provide Computer based and paper based procedures of a similar format, style and structure to minimise opportunity for confusion or justify an alternate approach.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-83	The licensee shall justify or remove the high usage of system designator codes in procedural information.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-84	The licensee shall provide and justify a place keeping system / methodology for procedural use that does not rely on operators marking up paper copies of computerised procedures.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

Annex 1

Assessment Findings to be Addressed during the Forward Programme as Normal Regulatory Business – Human Factors – AP1000

Assessment Finding Number	Assessment Finding	Report Section Reference	Timescale
AF-AP1000-HF-85	The licensee shall reassess the alarm threshold values in terms of their meaningfulness to operators and the application of standard engineering units rather than percentage of measurement ranges.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-86	The licensee shall consider operator support requirements relating to rectifying underlying problems associated with alarm messages and the permitted timescales for doing that.	4.6.7	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning
AF-AP1000-HF-87	The licensee shall provide arguments and evidence relating to the HF aspects of communications, the approach to emergency response and a Training Needs Analysis.	4.6.9	Mechanical, Electrical and C&I Safety Systems – Before inactive commissioning

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 – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

COMPLETENESS OF THE HUMAN FACTORS SAFETY CASE

GI-AP1000-HF-01 REVISION 0

Technical Area	**HUMAN FACTORS**		
Related Technical Areas	N/A		
GDA Issue Reference	**GI-AP1000-HF-01**	**GDA Issue Action Reference**	**GI-AP1000-HF-01.A1**
GDA Issue	Completeness of the Human Factors Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential.		
GDA Issue Action	Westinghouse submitted a significant volume of important HF analysis towards the end of GDA Step 4 relating to human error mechanisms, operator misdiagnosis and violation potential. ONR undertook a very high review of the submission to gain confidence in the approach, but was unable to undertake a detailed and thorough assessment within the Step 4 timescales. This GDA Issue Action requires Westinghouse to support ONR's full assessment of this submission; specifically Westinghouse should: • Provide adequate responses to questions raised from ONR assessment of documents submitted during Step 4. 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-AP1000-HF-01 Revision 0	Ref. 179.

Annex 3

Human Actions Selected for Detailed Assessment

No.	Type A	Type B	Type C
1	OPR-011: Maintenance error leads to ADS failing to vent RCS when required (Failure can be due to squib valves failing to open due to latent error, valves inappropriately left closed (stage 4), or piping is not properly vented)	OPR-004: SG level transients at low power result in reactor trip	ADN-MAN01: Operator fails to manually actuate the ADS
2	OPR-067: Maintenance error results in containment isolation valve stuck open	OPR-105: Miscalibration of plant stack radiation monitor	ATW-MAN03: Operator fails to manually trip the reactor through PMS in one minute
3	OPR-068: Mispositioned CIM prevents control signal from reaching an actuated component	OPR-130: Improper Latching of a Fuel Assembly	CIB-MAN00: Operator fails to diagnose SGTR
4	OPR-087: Maintenance error leads to damage of the containment hatch or airlock seal		CIB-MAN01: Failure to close MSIV on a ruptured SG
5	OPR-096: Maintenance error leads to failure of a PRHR air operated outlet isolation valves to open when required		CIC-MAN01: Operator fails to isolate containment
6	OPR-106: Maintenance error leads to failure of recirculation squib valves		CVN-MAN00: Operator fails to align CVS
7	OPR-109: IRWST level instrumentation miscalibrated or made inoperable, preventing automatic transfer to sump recirculation		CVN-MAN03: Operator fails to start CVS Pump B
8	OPR-127: Operator leaves CMT isolated following maintenance		FLISM: Auxiliary personnel fail to isolate or mitigate the flood (flood PRA)
9	OPR-129: CMT not vented or refilled following maintenance leaving some non-condensible gases		HPM-MAN01: Operator fails to diagnose need for high pressure heat removal
10	OPR-132: Foreign material left behind in the Core		LPM-MAN01: Operator fails to recognize the need for RCS depressurisation *(during a small LOCA or loss of high pressure heat removal system)*
11	OPR-150: PMS division left in partial or full bypass		LPM-MAN05: Operator fails to recognize the need for RCS depressurisation *(during a shutdown condition with failure of the CMTs and the RNS)*

Annex 3

Human Actions Selected for Detailed Assessment

No.	Type A	Type B	Type C
12	OPR-151: Improper restoration of CVS alignment following maintenance		OPA-02: Operator fails to open manual valve to sprinklers in containment (Fire PRA)
13	OPR-174: Maintenance error results in Pressuriser (PZR) Safety Valve incorrect opening set point (fails to open or opens prematurely)		PRN-MAN03: Operator fails to align/control PRHR system operation
14			REC-MANDAS: Operator fails to diagnose an event through DAS signals or perform an activity by operating DAS controls
15			REN-MAN02: Operator fails to initiate recirculation during LOCA
16			REN-MAN04: Operator fails to Initiate Recirculation (LOCA and IRWST level signal failure)
17			RHN-MAN01: Operator fails to align RNS
18			VWN-MAN01: Operator fails to align Standby Chiller (fails to recognise the need and fails to align the standby chiller during a LOCA).
19			ZON-MAN01: Failure to start on-site standby diesel generator.

Annex 4

Work Stream 1 - Detailed Action Assessment Proforma

This Proforma was used to record the assessment. The purpose of using a proforma was to facilitate comparison between assessments, and to provide assurance that each assessment has been undertaken in a consistent manner, considering similar factors.

OVERVIEW OF ASSESSMENT OF OPERATOR CLAIM	
Section 1	
Step 1: Claim	
Assessor Claim reference	
Section 2	
Step 2: Error Information	
Error Identifier	
Error Title	
Error Type	*e.g.: physical, manual, supervisory, diagnostic, monitoring, cognitive*
Error Consequence	
Error Frequency	*HEP*
Associated Safety System	
WEC proforma completed	
Step 3: Claim	
Description of Claim	*Clarify and record understanding of the claim.* • *What issues would you expect to see?* • *Understand and record the extent of the risk associated with the claims being made on the operator and hence form a view of the level of substantiation expected. This should take account of the level of the HEP, FV and Risk Importance Factor (RIF) values, and may also include assessor judgement.* • *Nature of task – understand the demands it makes on operators, etc.*
Step 4: Human Error Identification (HEI)	
HEI Method used	
Potential Logical Errors	
Viable Error Mechanisms	

Annex 4

Work Stream 1 - Detailed Action Assessment Proforma

OVERVIEW OF ASSESSMENT OF OPERATOR CLAIM	
Section 3	
Step 5: Qualitative Assessment *Consider the claimed action against each heading, as set out below. Where a heading is not considered significant for the claim, then 'Not Significant' can be recorded (e.g. where the claim is for stopping a pump in response to an alarm, then Training and Skill Levels might be considered not significant in comparison to time, equipment design, environment, etc.).* • *Is it applicable to the claimed action?* • *What has Westinghouse said?* • *Has Westinghouse conducted analysis (if not, is this acceptable?)* • *Has Westinghouse used an appropriate approach?* • *Has the approach been applied in an appropriate manner?*	
Saliency of Signals	*This is looking at the immediate prompts which are available for the operator to take the claimed action. Consider the following:* • *Alarms / warnings / indications / interfaces / communications* • *Compelling / 'attention- getting'* • *Masked signals* • *Good indication of what it is / action required*
Information available	*This is about the information available to support successful execution of the claimed action and in terms of availability and adequacy. This is not about cues to initiate claimed action (detection and diagnosis). This includes:* • *Procedures* • *Feedback* • *Instrumentation* • *Job Aids*
Time available (or perceived)	*This is about time available compared with time required for claimed actions.* • *Also need to consider location for claimed actions e.g. indication in MCR but action required in another location* • *Consider '30 minute rule'* • *Time pressure* • *Also consider perceived time stress, which may affect performance even when there is sufficient time available.*
Workload	• *Physical and cognitive demands*
Environment	*This is about considering the environment in which the claimed action is to be executed.* • *Consider 'normal' environment and 'fault/hazard' environments and the feasibility of the claimed action under the environment.* • *Lighting* • *Temperature* • *Noise* • *Space (access/egress)* • *Stress (need to consider whether the Westinghouse assessment has considered the potential for stress to affect performance during fault conditions)*

Annex 4

Work Stream 1 - Detailed Action Assessment Proforma

OVERVIEW OF ASSESSMENT OF OPERATOR CLAIM	
Operator Capabilities	*This is about if the operator can physically perform the task:* • *Force required* • *Hear the alarm, discriminate the tone* • *Colour vision* • *Physical workload (for specific claimed action)* *If the cognitive demands of the task have been identified and substantiated, including:* • *Mental workload (for specific claimed action)* • *Memory demands*
Work Design and Organisation	*This is about how the individual claimed action fits into the totality of all tasks being undertaken. Is the action feasible considering the work design, management and organisation, e.g.:* • *Staffing levels* • *Communications* • *Overall workload (over and under load)* • *Fatigue*
Training and Skills	*This is about gaining confidence that Westinghouse has sufficient understanding of the levels of skill and competence that are required reliably to execute the claimed action and hence to ensure that SQEP personnel will be available.* • *Availability of SQEP personnel given the level of skill and training required i.e. for those infrequent, highly skilled actions.*
Equipment Design	*This is about the physical equipment design of the equipment which is required to perform the claimed action, consider:* • *Anthropometry* • *Displays* • *Accessibility* • *Tools*
Step 6: HEP *Form and document your judgement about whether the derived HEP is reasonable and adequately substantiated. Consider:* • *Dependencies – how have they been modelled?* • *HEI output – have the relevant human errors been considered?* • *HEP derivation – has an appropriate method been applied appropriately, and is the resultant HEP reasonable and suitably substantiated?* • *Make a quantitative assessment of the impact of any performance shaping factors* • *Show details of all calculations,* • *Use the output from Step 6, above to inform the judgement.*	
HEP Process	
Performance Shaping Factors etc.	
Calculation	
Derived HEP	
Step 7: ALARP	
ALARP Comments	*Form a judgement, where possible, as to whether Westinghouse appears to have considered ALARP issues or whether there are indications that further risk reduction would be practicable.*

Annex 4

Work Stream 1 - Detailed Action Assessment Proforma

OVERVIEW OF ASSESSMENT OF OPERATOR CLAIM	
Section 4	
Step 8: Conclusions	
Specific to Claim	• *Has the claimed action been substantiated?* • *Was the substantiation performed adequate for the error and the risk associated with the error?* • *Are the methods appropriate for the error?* • *Does the HEP represent a realistic probability based on the information reviewed?* • *Does Westinghouse appear to have done everything reasonably practicable to reduce the risk?*
Generic	• *Does this assessment raise issues about Westinghouse process for substantiation?* • *Have these methods been applied in a systematic way?*
Assumptions *Ensure that all assumptions are captured as the assessment progresses.*	
Westinghouse	*Westinghouse – implicit and explicit assumptions that underpin their assessment*
Assessor	*Assessor – assumptions made in order to progress the assessment (consider whether it is appropriate to make an assumption, or to record a finding)*
Assessor's Additional Comments (if applicable)	

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
ADF-MAN01	Operator fails to depressurise the Reactor Coolant System (RCS) to refill the Pressurizer	C	The base HEPs for this claim are reasonable, but the recovery claims are considered over-optimistic. [Claim not substantiated]	The claims for recovery should be reconsidered and, if necessary, the HEPs should then be recalculated.
ADN-MAN01	Operator fails to manually actuate the ADS	C	There are qualitative concerns about the difficulty of diagnosis and the times required. The HEP is considered optimistic. [Claim not substantiated]	The diagnostic steps should be reconsidered and the HEPs should then be recalculated.
ATW-MAN03	Operator fails to manually trip the reactor through PMS in one minute	C	The timescales postulated for this task are too tight to provide confidence that the reactor could be manually tripped within a minute of an alarm for rods not all being at the bottom unless an *RO* had already entered E-0. If the *RO* had already entered E-0, this would be considered an optimistic claim. [Claim not substantiated]	For this HEP it would be more appropriate to start from the assumption that an *RO* had already entered E-0 and was anticipating a reactor trip. Consideration should be given to re-assessing the requirement for this task to be completed within one minute, to determine whether this timescale can reasonably be extended.
CCN-MAN02	Inadvertent misalignment of CCS Heat Exchanger	A	These tasks are likely to be undertaken quickly without comprehensive checking and so it is not justifiable to make any claims for recovery. This means that the HEPs are optimistic. [Claim not substantiated]	The claims for recovery should be reconsidered and, if necessary, the HEPs should then be recalculated.
CIB-MAN00	Operator fails to diagnose SGTR	C	The assessor considers that two steps have been omitted from this claim. Also, the recovery claims are considered optimistic. [Claim not substantiated]	The HEPs should be reassessed.
CIB-MAN01	Failure to Close MSIV on a Ruptured SG	C	The overall assessed HEP of 1.34×10^{-3} looks to be optimistic. With the exception of the requirement that an RO ensures that the MSIV Bypass Isolation Valve(s) SGS-V240A and/or SGS-V240B are closed, the HEI process appears to have considered the principal human errors that might be anticipated. [Further evidence required]	The claim of 1.34×10^{-3} does not take account of the in-built dependence between the apparent training of SROs and *RO*s, which could be expected to tip any probability of failure towards the higher end of the spectrum rather than the lower end.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
CIC-MAN01	Operator fails to Isolate Containment	C	In calculating a HEP of 5.71E-03, WEC do not identify any PSFs, other than stress. No explanation is provided as to why THERP, which is preferably for discrete tasks such as manipulating a dial, was used to assess a task that involves a sequence of requirements including monitoring, diagnosis and action execution. [Claim not substantiated]	The claim is, at face value, feasible: should automatic actuation of containment isolation fail, the operator will manually actuate the isolation. However, there are a number of factors which are unclear which lead to the conclusion that, currently, the claim cannot be, and has not been, substantiated.
CVN-MAN00	Operator fails to align CVS	C	The claims for recovery are optimistic, but their impact is limited. [Claim substantiated]	Claim is reasonable.
CVN-MAN03	Operator fails to start CVS Pump B	C	There is conflicting information within the HRA, such that confidence in the assessed HEP of $1.07x10^{-3}$ is low, because there does not seem to be sufficient understanding of the task. [Claim not substantiated]	There is no discussion, or apparent consideration, of dependency, which would be expected when claiming supervisor intervention.
FLISM	Auxiliary personnel fail to isolate or mitigate the flood (flood PRA)	C	The use of THERP to derive an indicative HEP of $3.8x10^{-2}$ appears reasonable, providing the plan is a good one and gets the Auxiliary Personnel to the right place, at the right time. [Claim substantiated]	WEC's HEP assessment does not appear to consider dependencies, of which there might be more than a few, especially if, as would seem likely, diagnosis of the problem and developing an immediate and effective plan to deal with this, had to be developed at short notice.
HPM-MAN01	Operator fails to diagnose need for high pressure heat removal	C	It was considered that each of the base HEPs were inappropriate and optimistic. Furthermore, all the recovery claims were also optimistic. [Claim not substantiated]	The claims for recovery should be reconsidered and then the HEPs should then be recalculated.
LPM-MAN01	Operator fails to recognize the need for RCS depressurisation (during a small Loss Of Coolant Accident (LOCA) or loss of high pressure heat removal system)	C	The claim for an error of omission is too optimistic and this optimism is further increased by the recovery mechanisms that are used. [Claim not substantiated]	The HEPs for the error of omission should be reconsidered and the recovery mechanisms should be amended.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
LPM-MAN05	Operator fails to recognize the need for RCS depressurisation (during a shutdown condition with failure of the CMTs and the RNS)	C	The assessed reliability of 6.83×10^{-4} is grossly optimistic. The assessment fails to take account of the large number of intervening steps required before the essential plant interactions are reached. It is suggested that the probability of misdiagnosis, notwithstanding the detection of low hot leg water level will be high. [Claim not substantiated]	These HEPs should be re-assessed.
OPA-02	Operator fails to open manual valve to sprinklers in containment (Fire PRA)	C	Unless there are compelling arguments to suggest that breathing apparatus will never be necessary in this situation, it is concluded that this manual de-isolation is unlikely to be feasible within 30 minutes. In this case the overall assessed HEP of 3.0×10^{-2} should be amended and set at unity. [Claim not substantiated]	Consideration should perhaps be given to automating the operation of the Fire Water Containment Supply Isolation Valve (FPS-V050) so that it can be opened remotely from the MCR. If this is not possible, the current procedural instruction within AOP 305 should be rewritten so that it is less ambiguous and can be used by a member of a rescue team who is not familiar with the plant.
OPR-004	SG level transients at low power result in reactor trip	B	The provision of an automated flow controller for Start up Feedwater and its integration with the Main Feedwater flow controller should reduce the requirement to manually control the SG flows, especially during startups and shutdowns, when inadequate manual control can lead to an inadvertent reactor or turbine trip. [Claim substantiated}	The argument for WEC's approach is that inadvertent reactor trips when the SG levels are being controlled manually will be the same as, or fewer than they are in current PWRs. This argument is upheld.
OPR-011	Maintenance error leads to ADS failing to vent RCS when required (Failure can be due to squib valves failing to open due to latent error, valves inappropriately left closed (stage 4), or piping is not properly vented)	A	The HEP appears optimistic and is not substantiated by sufficient qualitative analysis. [Claim not substantiated]	Lack of completeness in claims makes this difficult to assess or conclude that the claim is substantiated by suitable analysis.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
OPR-067	Maintenance error results in containment isolation valve stuck open	A	Task and mechanism by which error might occur not clearly defined. General description of the *HFE* could hide a specific valve that is not fully covered by WEC's considerations. [Further evidence required]	Likely that the indications and testing of these valves, given their important role, can be substantiated.
OPR-068	Mispositioned CIM prevents control signal from reaching an actuated component	A	An HEP of 6.0×10^{-5} would not be unreasonable if the barriers discussed were in place (i.e. no dependencies, etc.). Insofar as the arrangements implied in the WEC analysis can be determined, the numbers are at the optimistic end, but it is, nevertheless, plausible. The time at risk and error correction potential do not seem to have been considered. [Claim not substantiated]	The analysis is credible for routine maintenance but the connection between HRA and HF could be closer. If this error were to occur in emergency conditions, then a different HEP would be applicable.
OPR-087	Maintenance error leads to damage of the containment hatch or airlock seal	A	The claim does not appear to be well-substantiated, WEC has not provided any analysis of the required leak test procedure or discussion of how the seals may be damaged. [Claim not substantiated]	As no proforma has been developed for this HEP, the information within the summary does not clearly define the task and the mechanism by which this error might occur.
OPR-096	Maintenance error leads to failure of a PRHR air operated outlet isolation valves to open when required	A	HEP of 6.45×10^{-5} would require robust task design, independent verification, opportunity for independent error identification, record of system configuration and opportunity for recovery. [Further evidence required]	Dependency has not been addressed with reference to this task, but the claim appears reasonable and it could be substantiated in due course. However, WEC has not yet demonstrated this.
OPR-099	Operator incorrectly executes the Coolant Makeup Tank (CMT) discharge valves operability test	B	The claim appears reasonable, but there is insufficient information to substantiate it. [Claim not substantiated]	More evidence required in order to properly assess this HEP.
OPR-105	Mis-calibration of plant stack radiation monitor.	B	The claim appears reasonable in general and it could well be substantiated, in due course. However, WEC has not provided any information or any substantiation of the task because the current HFA safety case is limited to CDF risk only, and, therefore, this action does not have a proforma. [Claim not substantiated]	Even though an HEP has not been calculated for this Action/*HFE*, WEC do not seem to have considered the potential and the consequences of the plant stack radiation monitor being set too low and causing un-required closure of the discharge system.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
OPR-106	Maintenance error leads to failure of recirculation squib valves.	A	HEP of 6.45×10^{-5} would require robust task design, independent verification, opportunity for independent error identification, record of system configuration and opportunity for recovery. [Claim not substantiated]	It is not clear, from the information provided, that such a high reliability can be demonstrated for this error.
OPR-109	IRWST level instrumentation mis-calibrated or made inoperable, preventing automatic transfer to sump recirculation.	A	HEP calculation is very high level and there has not been adequate breakdown of the subtasks to identify specific requirements of tasks and associated errors. [Further evidence required]	The claim appears reasonable and it could be substantiated in due course.
OPR-127	Operator leaves CMT isolated following maintenance.	A	The claim seems optimistic. Unclear whether all the valves that could result in CMT unavailability have been considered in terms of their indication in the MCR and their inclusion in a surveillance regime. [Further evidence required]	WEC assumption of maintenance once/year needs confirming, as it appears that these valves are manipulated more than for maintenance alone.
OPR-129	CMT not vented or refilled following maintenance leaving some non-condensible gases.	A	There has not been an adequate breakdown of the subtasks to identify the specific requirements of the tasks and the associated errors. The HEP of 4.76×10^{-6} calculation is very high level. [Further evidence required]	Clear demonstration of the fault sequences, with individual HEPs derived and placed into the fault sequence is not evident. However, the claim appears reasonable and it might be possible to substantiate it, in due course.
OPR-130	Improper latching of fuel assembly.	B	The categorisation of the Refuelling Machine Operator's check is optimistic and it is not appropriate to use a different classification for the Supervisor's check. Therefore, this claim is considered unreasonably optimistic. [Claim not substantiated]	There will be dependency between these two checks, but this should be modelled more directly, and not by using a different task for the Supervisor's check.
OPR-132	Foreign material left behind in the core.	A	The HEP of 6.0×10^{-5} appears optimistic and is not substantiated by sufficient qualitative analysis. The calculation is mathematically accurate but takes no account of any potential dependency between the initial error and the check. [Claim not substantiated]	It is quite possible that the error of foreign materials being introduced and the subsequent consequence of fuel becoming ledged on that material are independent, but it is not possible to judge this based on the information provided.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
OPR-150	PMS Division left in partial or full bypass	A	There is insufficient evidence provided to assess this claim or the impact of any postulated error mechanisms. [Claim not substantiated]	More evidence required in order to properly assess this HEP.
OPR-151	Improper restoration of CVS system alignment following maintenance.	A	There appear to be a number of potentially different mechanisms by which the CVS could be misaligned following maintenance, each of which could have been assessed separately. [Further evidence required]	When no proforma is completed the information provided by WEC is minimal such that it is difficult to conclude that the claim is substantiated.
OPR-174	Maintenance error results in PZR Safety Valve incorrect opening set point (fails to open or opens prematurely)	A	Claimed HEP of 6.0×10^{-5} made for operator reliability in relation to OPR-174 is not substantiated by the available actuarial evidence. [Claim not substantiated]	The exact nature of the tasks to be performed in order to set Pressurizer lift setpoints correctly need to be re-examined by WEC and better account taken of actuarial data.
OPR-179	Operator erroneously causes inadvertent operation of ADS	B	The claim by WEC exceeded the HPLV, but otherwise it was substantiated. [Claim substantiated, but considered optimistic]	Consideration should be given to developing an HPLV for AP1000 and then applying it to this HEP.
PRN-MAN03	Operator fails to align/control PRHR system operation	B	The claims for preventing omission errors are optimistic and the overall claims are then made more optimistic by the recovery factors that have been used. [Claim not substantiated]	The claims for recovery should be reconsidered and, if necessary, the HEPs should then be recalculated.
REC-MANDAS	Operator fails to diagnose an event through DAS signals or perform an activity by operating DAS controls	C	WEC claim that the highest independent HEP of 1.16×10^{-2} is chosen to represent REC-MANDAS and that this is viewed as a conservative HEP for DAS actuation of all systems. WEC do not provide a rationale, or evidence, as to why this is a 'conservative' HEP. [Further evidence required]	Conceptually, ATW-MAN04 and ATW-MAN06 are similar, if not identical, to REC-MANDAS, but neither of these has a proforma, whereas REC-MANDAS does.
REN-MAN02	Operator fails to Initiate Recirculation during a LOCA.	C	The overarching conclusion of this assessment is that WEC's sentencing of this claim, as not requiring further analysis through a Proforma, appears flawed. [Claim not substantiated]	Because the claim was not deemed significant enough for a Proforma, there is limited information to assess to identify if the substantiation was sufficient. This leads to the conclusion that the substantiation was not sufficient, as it was not performed.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
REN-MAN04	Operator fails to Initiate Recirculation (LOCA and IRWST level signal failure)	C	$4.77x10^{-3}$ (A HEP of $1.0x10^{-2}$ is used for this operator action in the PRA quantification). The resultant HEP is not reasonable or suitably substantiated. [Claim not substantiated]	This operator error needs reassessment using more sophisticated HEI methods which take account of the realities of trying to perform a diagnostic task without very effective indications, in a UK context.
RHN-MAN01	Operator fails to align RNS	C	It appears that at least two control actions will be necessary to align the RNS valves and a further action will be required to start the RNS pumps. These additional two tasks and the potential for omission errors associated with them would greatly increase opportunities for error and mean that the HEPs produced by WEC are optimistic. [Claim not substantiated]	Information that was available about the nature of tasks underlying this assessment appeared limited and interpretation of task requirements suggested that WEC's assessment may have been based upon an incomplete and inaccurately defined set of tasks. Therefore, these HEPs should be reassessed.
RHN-MAN05	Operator fails to initiate gravity injection from IRWST via RNS suction line	C	Despite its stated relative unimportance, this action was of sufficient concern at the time of the preparation of the HRA, for considerable time and effort to be devoted to assessing the scenario and trying to assign some estimates to the likelihood of failure. I consider the resulting HEP to be optimistic, and hence it may prove to be misleading in practice. [Claim not substantiated]	The precise nature of the task and the context in which it might have to be performed needs to be better understood, together with the risks that might arise and these need to be reassessed and demonstrated to be ALARP.
SGA-MAN01	Inadvertent opening of SG Power-Operated Relief Valve	B	The individual HEP descriptors and values are realistic and seem appropriate. However, the overall HEP of $2.35x10^{-6}$ is very optimistic and should be reduced to the HPLV. [Claim substantiated]	Consideration should be given to developing an HPLV for AP1000 and then applying it to this HEP.
VWN-MAN01	Operator fails to align Standby Chiller (fails to recognise the need and fails to align the standby chiller during a LOCA).	C	The HEP claim of $5.16x10^{-3}$ was optimistic and is called into question as the validity of qualitative and quantitative modelling was inadequate. [Claim not substantiated]	This HEP should be reassessed.

Annex 5

Work Stream 1 - Summary of Assessment of Human Actions

HAD ID	Descriptor	Error Type	Summary	Implications
ZON-MAN01	Failure to start on-site standby diesel generator.	C	The claimed HEP is optimistic qualitatively, because relevant actions that are pertinent to starting essential supplies appear to be omitted, especially the diagnosis of automated diesel start failures and load shedding or sequencing failures. The claim is quantitatively optimistic because claims on alarm detection are optimistic, whilst recovery claims are inappropriate and over-optimistic. [Claim not substantiated]	The underlying tasks should be re-examined and then the HEPs should be reassessed.

Annex 6

Work Streams 1 and 3 – Recalculation of Squib Valve maintenance task human error potential (OPR-011)

Original Westinghouse calculation – OPR-011

Initial maintenance failure – HEART GTT F *"Restore or shift a system to original or new state following procedures, with some checking……."* = nominal HEP $3.0x10^{-3}$ (no Error Producing Conditions (EPCs) applied)

Pre start-up visual checks failure – HEART GTT E *"Routine, highly-practised, rapid task involving relatively low level of skill……."* = nominal HEP $2.0x10^{-2}$ (no EPCs applied)

Overall Westinghouse EC calculated HEP - $3.0x10^{-3}$ x $2.0x10^{-2}$ = $6.0x10^{-5}$ (Westinghouse calc number 3, see Ref. 35 Table 4-7 and section A.5.4)

ND calculation

Initial maintenance failure – HEART GTT F = nominal HEP $3.0x10^{-3}$

I agree with Westinghouse that GTT F task descriptor provides a suitable representation of the maintenance task; given current understanding.

Given the infrequency with which such maintenance tasks are likely to be performed it is considered appropriate to apply HEART EPC 1 which addresses unfamiliarity; "*Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel"*. This EPC carries a maximum weighting effect of x17. However, while the task is considered to be unfamiliar it will not be wholly thus and therefore an Assessed Proportion of Effect (APoE) of 0.25 is applied. I am satisfied that other potential EPCs such as a shortage of time or a low signal to noise ratio in the assembly tasks are unlikely.

(17-1) x 0.25 + 1 = 5

$3.0x10^{-3}$ x 5 = $1.5x10^{-2}$

Pre start-up visual checks failure – HEART GTT C *"Complex task requiring a high level of understanding and skill……"* = nominal HEP $1.6x10^{-1}$

I have selected HEART GTT C in place of Westinghouse's selection of GTT E as I disagree that the checking activity is likely to be a "*routine, highly practised, rapid task"*. As per the HEART GTT descriptor GTT E relates to distantly mission oriented tasks involving typically *"a single discrete element or action"*. I do not understand this to be the case for the checking task modelled here. GTT C has been selected to take account of the likely complexity of the task such that the checker will be required to understand the various components of the device and their correct assembled state in order to perform the check effectively.

As with the maintenance task itself the infrequency with which the checking task is likely to be performed necessitates the application of HEART EPC 1. Also as for the maintenance task an APoE of 0.25 is applied. I am satisfied that other potential EPCs such as a shortage of time or a low signal to noise ratio in the assembly tasks are unlikely.

(17-1) x 0.25 + 1 = 5

$1.6x10^{-1}$ x 5 = $8.0x10^{-1}$

I have also considered the possibility for dependency within my assessment using the THERP dependency model. As the checking activity is stated by Westinghouse to be *"Pre Start-up"* it is reasonable to assume that this will be performed some time after the actual maintenance activity, although this is not explicitly stated. It is also assumed for this assessment that the checks are performed by alternate personnel from those who undertook the maintenance. Despite these considerations I feel it is still appropriate that a Low level of dependence is modelled between the maintenance task and the subsequent checks.

Applying the THERP dependence model for 'Low' dependence modifies the HEP for the checking task to 8.1E-1. Therefore the overall HEP for the activity is reassessed as:

$1.5x10^{-2}$ x $8.1x10^{-1}$ = $1.2x10^{-2}$