Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 HUMAN FACTORS ASSESSMENT OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/021-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This report presents the findings of the Human Factors (HF) assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process.

This report for AP1000 presents the results of my Step 3 assessment of HF. It provides an overview of the safety case presented in the PCSR; the standards and criteria adopted in the assessments; and an assessment of the human based safety claims as presented in the safety case.

The scope of the HF assessment is detailed in the Project Initiation Document (PID) (Ref. 5) which states that the GDA Step 3 HF assessment will be more aligned to the level of detail undertaken during GDA Step 2 (focused on the safety 'claims'), due to the delayed commencement of the ND assessment in HF (June 2009).

The approach to the assessment of HF was to confirm that the Westinghouse PCSR clearly presents the contribution of human actions to safety. This formed the focus of my assessment. In addition assurance was sought that Westinghouse has HF analysis to support the human based safety claims (for assessment during GDA Step 4); that the age of this supporting analysis is not a detriment to their risk assessment when compared to modern standards; that the standards used are appropriate and that there has been an adequate integration of HF into the NPP design and PCSR and supporting documents.

Westinghouse HF safety arguments are set out in the PCSR, which essentially refers out to Chapter 18 of the AP1000 European Design Control Document (DCD) (Ref. 6). Chapter 18 of the DCD (Human Factors Engineering) describes the process and scope of HF work undertaken and references out to lower tier documents. The PCSR and DCD do not present analysis and argument in a structure that provides a clear identification of the 'claims, arguments and evidence', and they do not present an overview of the human based safety claims or clearly highlight what the human contribution to safety is for the AP1000. This has presented me with difficulties in the area of HF considering that my assessment strategy for GDA Step 3 is focused on safety 'claims'. I am also limited in my ability to progress my assessment, as my strategy for GDA Step 4 will be to target my focus on a proportionate basis to those areas where the human contribution to safety is greatest.

As part of our work on the Probabilistic Safety Analysis (PSA) Human Reliability Analysis (HRA) I have some transparency on the human contribution to safety; however concerns on the scope and quality of the PSA have been raised in the GDA Step 3 PSA assessment (Ref. 10). Therefore, at this time I have no confidence that the PSA presents a complete understanding of the human contribution to safety. Furthermore, the HF analysis and argument does not appear to be fully integrated with the PSA work.

I have made several attempts to help bridge what I consider to be a knowledge gap on the part of Westinghouse in terms of UK expectations for safety case presentation, but with limited success to date. However Westinghouse has now committed to developing a safety case in the area of HF, and has provided a programme of work using suitably qualified and experienced personnel, aimed at meeting UK regulator expectations. It is with this commitment that I recommend progression of the AP1000 to Step 4 of the GDA process in the area of HF. However it is important to highlight that unless an adequate safety case for HF is delivered early on in GDA Step 4, this topic is likely to progress to a Regulatory Issue.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As low as reasonably practicable
ATWS	Anticipated Transient Without Scram
BMS	(Nuclear Directorate) Business Management System
CDF	Core damage frequency
CMT	Core Make-up Tank
CNSC	Canadian Nuclear Safety Commission
CSF	Critical Safety Functions
DAS	Diverse Actuation System
DBA	Design Basis Analysis
DCD	Design Control Document
EA	Environment Agency
GDA	Generic Design Assessment
HCI	Human Computer Interaction
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Events
HFI	Human Factors Integration
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSE	The Health and Safety Executive
HSI	Human System Interface
IAEA	The International Atomic Energy Agency
IRWST	In-containment Refuelling Water Storage Tank
LOCA	Loss of Coolant Accident
MDEP	Multi-national Design Evaluation Programme
ND	The (HSE) Nuclear Directorate
NPP	Nuclear Power Plant
PCSR	Pre-construction Safety Report
PID	Project Initiation Document
PMS	Plant Monitoring System
PSA	Probabilistic Safety Analysis
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
RCS	Reactor Coolant System

LIST OF ABBREVIATIONS

RI	Regulatory Issue
RIA	Regulatory Issue Action
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
SAP	Safety Assessment Principle
SGTR	Steam Generator Tube Rupture
SQEP	Suitably Qualified and Experienced Personnel
SSC	System, Structure and Component
TSC	Technical Support Contractor
US NRC	The United States Nuclear Regulatory Commission
WEC	Westinghouse Electric Company LLC
WENRA	The Western European Nuclear Regulators' Association

TABLE OF CONTENTS

1 INTRODUCTION

1 This report presents the findings of the Human Factors (HF) assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the HSE Generic Design Assessment (GDA) process. This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 2) and its associated guidance document G/AST/001 (Ref. 3). AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 4) have been used as the basis for the assessment of HF associated with the AP1000 design. The SAPs require that human factors issues on a Nuclear Power Plant (NPP) or nuclear chemical plant site be identified and considered in safety assessments. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 The approach taken to the HF assessment for GDA Step 3 was more aligned to the level of detail undertaken for GDA Step 2; focused on the safety 'claims', with some amplification. There was no HF assessment work undertaken for GDA Step 2, and assessment work did not commence until June 2009, resulting in the HF technical assessment programme being significantly behind other disciplines.

3 The scope of the assessment for HF is detailed in the ND Project Initiation Document (PID) (Ref. 5) which states that the main focus will be on identifying the human based safety claims to gain an understanding of the human contribution to safety. In addition I have assessed the availability and age of supporting analysis (or substantiation), judged the appropriateness of the standards applied and considered the adequacy of the level of Human Factors Integration (HFI).

4 It should be noted that due to the delayed start of the HF assessment and the sampling nature of our work, not all aspects of the assessment scope have been covered in the same level of detail.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

5 The HF aspects of the PCSR are detailed in the following sections of the PCSR:

- 8.4: Human Factors Modelling in Support of DBA;
- 8.5.6: Dependence on Operator Action; and
- 9.5.8.5: Human Factors Enhanced Control Room.

These sections form the totality of the HF content of the Westinghouse PSCR for the AP1000. (I note that there is also Section 11.12 which provides a paragraph dealing with HF in relation to operational aspects, but it merely states that this is a matter for the operating organisation.)

6 Section 8.4 of the PCSR provides a description of *"five Design and Implementation activities"* which form the HF engineering programme. These are:

- Planning.
- Analysis (including functional requirements analysis and functional allocation; task analysis; staffing; and human reliability analysis).
- Design (including interface design; procedure development; training development; and verification and validation).
- Operation (including design implementation and human performance modelling); and

- Probabilistic Risk Assessment.

7 Under each of these headings there is essentially a simple paragraph description of what each work item aims to achieve, with no further amplification.

8 Section 8.5.6 of the PCSR provides a paragraph titled *"dependence on operator action".* This paragraph provides limited information on the results of sensitivity analyses and risk increase factor work on the PSA, which Westinghouse assert shows *"that the AP1000 has significantly less dependence on operator action to reduce plant risk to acceptable levels than current plants"*. In addition it is asserted that the human actions modelled in the PSA are *"generally simple…..easier and less likely to fail"*. Reference is also made to the human contribution to Core Damage Frequency (CDF).

9 Section 9.5.8.5 of the PCSR provides information relating to the *"human factors enhanced control room",* and this section appears to be the main focus of the HF contribution to the PCSR. The section provides a very limited description of the purpose and content of the control room, and cites advantages and disadvantages resulting from the HF engineering programme.

10 The PCSR further states that the detail of the HF engineering programme is discussed in Chapter 18 of the AP1000 European Design Control Document (DCD) (Ref. 6). Chapter 18 aims to describe *"the application of the human factors engineering disciplines to the design of the AP1000"*. It highlights that the basis of the Westinghouse HF engineering programme is the United States Nuclear Regulatory Commission (US NRC) prescription for HF engineering programmes – NUREG-0711 (Ref. 7). Also of interest is the citation that a number of the references highlighted were developed for the AP600 US NRC design certification (carried out in the mid 1990s), and that these references are asserted to be applicable to AP1000.

11 Chapter 18 essentially describes the HF engineering programme; its management, goals, applicability, composition, placement and authority of the team, roles and responsibilities, team qualifications, general processes and procedures, scope of work including the documents produced and the integration with other technical disciplines.

12 Limited detail is then provided on the individual work items (i.e. the scope of the HF engineering programme), and this simply involves a description of the work item and what it aims to achieve, a reference to the individual report providing the analyses, and a description of the scope of work of the analyses. Scope descriptions are provided for functional requirements analysis and allocation; task analysis (including operational sequence analysis and workload analysis); staffing levels and qualifications of plant personnel; integration of Human Reliability Analysis (HRA) and HF engineering; human system interface design (including the AP1000 alarm system, the computerised procedure system and testing activities); HF design for the *"non-human-system interface portion of the plant"* (including maintainability, communications and environmental considerations; procedure development; training programme development and HF engineering verification and validation).

13 The majority content of Chapter 18 is dedicated to the AP1000 human system interface design work, and there is some attempt to link aspects of the HF engineering programme and provide a context; for example *"Staffing assumptions, operating experience reviews, functional requirements analysis and allocations, task analysis and integration of human reliability analysis provide the bases for identifying the human system interface requirements needed to support human functions and tasks"*. There is also some attempt at providing a safety context; for example *"The human system interface, which includes the integration of Safety Parameter Display System requirements, is designed to reduce the likelihood of operator error and provide for error detection and recovery capability for the identified critical human actions and risk important tasks"*. Furthermore, there is a link between the design basis and minimum inventory (a US requirement for dedicated or

fixed position displays and controls used to monitor the status of safety critical functions and to manually activate the safety related systems that achieve the critical safety functions). Although there is no requirement in the UK relating to minimum inventory, the focus on and link between safety significance and HF engineering/design is recognised and expected.

14 However the focus remains on providing a description of the discrete work items that form the scope of the human system interface design, with reference to lower tier material. Additional information is presented to describe the purpose (mission) of the main control room, the remote shutdown workstation, the technical support centre, the operations support centre, the Radwaste Control Area, local control stations and the emergency operations facility.

15 Chapter 18 does provide a section titled '*Probabilistic Risk Assessment and Safety Critical Human Actions';* and it is here that I would expect to see a full citation of the human based safety claims. However the description of this work item states that the focus was to identify the minimum inventory required to support '*critical human actions'* (refer to para. 13 of this report). This section further adds that *"there are no specific pre-planned, manually-controlled actions required for the safety-related systems to mitigate design basis events in the AP1000 design".*

2.2 Standards and Criteria

16 The Safety Assessment Principles (SAPs) have formed the basis of the HF assessment of the AP1000. The SAPs recognise that *"…the human contribution to nuclear safety can be positive or negative, and may be made during facility design, construction, operation, maintenance, and decommissioning"*. They require that *"a systematic approach to understanding the factors that affect human performance, and minimising the potential for human error to contribute to faults should therefore be applied throughout the entire facility life-cycle. 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 into account their differing capabilities and limitations. The assessments should demonstrate that the interactions between human and engineered components are fully understood, and that human actions that might impact upon nuclear safety are clearly identified and adequately supported."*

17 The principal SAPs relevant to this stage of the HF assessment are:

EHF.1 A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the facility lifecycle.

EHF.2 When designing systems, the allocation of safety actions between human and technology should be substantiated and dependence upon human action to maintain a safe state should be minimised.

EHF.3 A systematic approach should be taken to identifying human actions that can impact on safety.

EHF.10 Risk assessments should identify and analyse human actions that might impact on safety.

SC.4 A safety case should be accurate, objective and demonstrably complete for its intended purpose.

EKP.3 A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several layers of protection.

EKP.5 Safety measures should be identified to deliver the required safety function(s).

ESS.8 A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.

FA.9 Design Basis Analysis (DBA) should provide an input to the safety classification and engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.

FA.13 The PSA model should provide an adequate representation of the site and its facilities

FA.14 PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.

18 The latest revision of the SAPs is consistent with IAEA Standards and the WENRA Reference Levels (Ref. 8). In addition ND Technical Assessment Guides (TAGs) provide an interpretation of the SAPs, and have been applied to my assessment where relevant. For GDA Step 3 I have applied TAGs in the area of Human Factors Integration (HFI) [Draft], Early Initiation of Safety Systems, and Guidance on the Demonstration of ALARP (Ref. 9).

19 The UK also applies the fundamental principle of reducing risk to As Low As Reasonably Practicable (ALARP). This principle is at the forefront of 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 (Ref. 9) which states that *"the good practice or standard should be up-to-date, taking account of the current state-of-the-art: any practice or standard more than a few years old, or not subject to active on-going monitoring and review or not written by acknowledged experts may be suspect"*.

2.3 Nuclear Directorate Assessment

20 The approach taken to the assessment of HF for GDA Step 3 is more aligned to the level of detail undertaken for GDA Step 2; focused on the safety 'claims' with some amplification, as no HF assessment work had been undertaken on the AP1000 until June 2009. As a result there are no considerations or output from GDA Step 2 to form the basis of this assessment for GDA Step 3.

21 My assessment has been undertaken with the assistance of Technical Support Contractors (TSCs), and it is important to note that due to the sampling and targeting nature of assessment, not all aspects of my assessment have been covered in the same level of detail.

2.3.1 Observations on the Strengths of the PCSR and DCD

22 The DCD provides an overview of the HF engineering programme and processes from a descriptive perspective. This provides a level of confidence that the type of HF analysis work expected should be available for assessment in GDA Step 4. Chapter 18 of the DCD also provides a link via reference citation to the standards that have been applied and to the documents where the detailed HF analysis work is reported. From a brief consideration of the scope of the references, it appears that Westinghouse has a firm basis for the 'evidence' phase of assessment (GDA Step 4).

2.3.2 Observations on the Weaknesses of the PCSR and DCD

23 The PCSR and DCD do not present the safety case for HF for the AP1000, and at the end of GDA Step 3 I consider that Westinghouse has not presented an adequate safety case for the HF aspects of the AP1000. The documentation presented for assessment does not provide a clear identification of the claims, arguments and evidence, and indeed there is no analysis or argument cited at all in the relevant extracts of the PCSR and DCD.

24 There appears to be a complete reliance on the US regulatory approach (prescriptive) with frequent reference to Regulatory Guides and specific NRC requirements and criteria, which has little relevance to the UK regulatory regime (which is goal setting rather than prescriptive).

25 Detailed HF analysis is referenced, but the PCSR and DCD do not present the output of the HF work in a safety or risk framework, therefore although it appears that the type of detailed analysis work that I would expect is available, it is difficult to understand what safety relevance and contribution it has.

26 The majority of my assessment has relied on the HRA and PSA to gain some understanding of the human contribution to safety. I would have expected Westinghouse to have used this work as a starting point for the development of their UK safety case for HF, to provide them with a (human based) safety claims position, from which the arguments and evidence detailed in their HF analyses could flow.

2.3.3 Identification of the Human Based Safety Claims

27 This was the main focus of my assessment and fundamental to a safety claims based assessment strategy. Clarity on the human based safety claims provides confidence that Westinghouse fully understands the human contribution to safety and where human error can present a safety challenge, and that it has targeted their HF engineering and safety analysis work appropriately. This in turn provides a mechanism for Westinghouse to demonstrate that the risks from human error have been reduced to ALARP. Furthermore, precision on the human based safety claims ensures that key assumptions and requirements can be transferred and understood by the licensee organisation, and be translated into the operating regime (training and procedures for example).

28 Transparency on the human based safety claims enables me to target my subsequent assessment work (for GDA Step 4) on a proportionate basis to the human contribution to safety. This aspect of my assessment sought assurance that the PCSR / DCD provide a complete statement on the human based safety claims. This should include:

- the potential for latent human failures induced through maintenance, calibrations, inspection and testing;
- requirements associated with plant alignments, active monitoring and control and contributors to initiating events; and
- post fault operator requirements including fault diagnosis, manual activation of systems, detection of automatic system failure, manual back up of systems and initiation of the emergency plan.

29 Ordinarily the PSA model (if complete) and the fault schedule would provide a mechanism for extracting the human based safety claims. However at the time of writing there was no fault schedule available for the AP1000 and our assessment of the PSA highlights that not all expected human failure events (HFEs) have been modelled (Ref. 10).

30 Westinghouse states in the DCD that the AP1000 has been designed to significantly reduce the reliance on active safety systems to mitigate faults, and uses passive safety

systems that generally result in a reduced reliance on reliable human action post fault. However this should be demonstrated via analysis, to provide clarity on what human actions are required for safety. In addition I would expect that although there may be a reduced reliance on reliable post fault operator actions (assuming the potential for mis-diagnosis has been discounted via analysis), the requirements for human reliability become focused on maintenance type activities.

31 There is no complete citation of the totality of human based safety claims in the PCSR or Chapter 18 of the DCD.

32 Throughout my interactions with Westinghouse to date it has not been able to present either a complete or partial listing of the human based safety claims for the AP1000, and have been unclear on this expectation. I consider their knowledge and experience of UK expectations for HF inclusion into safety cases almost completely lacking. In my opinion this is a significant weakness as I cannot be confident that Westinghouse understands the human contribution to safety for the AP1000. This in turn presents doubts that the design of the AP1000 has fully considered the potential for human error, which may affect the overall risk.

33 I have worked with ND's PSA assessor and through our own assessment of the PSA and HRA (i.e. not relating to the PCSR HF aspects or Chapter 18 of the DCD) we have been able to gather some understanding of the human contribution to safety. Using this work we have determined that:

- No Type A HFEs (pre-fault errors degrading safety systems, e.g. misalignments and miscalibrations) have explicitly been included in the PSA model.
- Type B HFEs (human errors contributing to initiating events) appear to have been addressed to some extent but it seems that they have been considered mostly implicitly. It is not yet clear whether this is also the case for the Shutdown PSA since Chapter 54 of the AP1000 PRA Report (Ref. 11) does not document the derivation of the low power and shutdown initiating events. Explicit analysis of Type B HFEs is generally performed for low power and shutdown modes. This is particularly important since previous reactor designs have shown an increased vulnerability to human errors contributing to key initiating faults during low power and shutdown operational states. I will follow this up during GDA Step 4.
- For post fault operator actions, Ref. 12 presents a tabular listing of those HFEs modelled in the PSA which were selected for human factors task analysis. This table is reproduced in Table 1 of this report. There are further post fault operator actions modelled in the PSA, but it appears that these have not been considered from a HF perspective. The listing of HFEs selected for task analysis is stated to have been derived from the PSA importance analysis and an expert panel. I have not assessed in detail whether the extent of the task analysis work has been sufficient to address all the risk significant HFEs, however an initial look at tables 50.7 and 50.8 of Ref. 11 suggests that there are a number of relatively important HFEs for which task analysis has not been undertaken. For example HFEs LPM-MAN2, CVN-MAN00, OTH-SDMAN, RHN-MAN1 have Risk Achievement Worth (also known as Risk Increase Factor) above 1.7 but have not been included in the table reproduced below. I will take this forward during my Step 4 assessment.

Table 1: List of Post Fault Operator Actions Modelled in the AP1000 PSA and Selected for HF Analysis

	Basic Event ID	Basic Event Description
1	ADF-MAN01	Failure to depressurize the RCS to stop RCS leak using the first stages ADS valves, given failure of aux. spray during SGTR
2	ADN-MAN01	Failure to actuate the ADS for RCS depressurisation as recovery from failure of automatic actuation or for manual ADS actuation
3	ADN-MAN01C	Conditional probability of AND-MAN01
4	ATW-MAN04	Failure to recognise the need and failure to manually trip the reactor (through the PMS) in one minute, given ATWS
5	ATW-MAN04C	Conditional probability of ATW-MAN04
6	ATW-MAN05	Failure to recognise the need and failure to manually trip the reactor (through the PMS) in seven minutes, given ATWS
7	CIB-MAN00	Failure to diagnose a steam generator tube rupture event
8	CIB-MAN01	Failure to close main steam isolation valve to isolate the faulted steam generator, given a steam generator tube rupture event
9	IWN-MAN00	Failure to recognise the need and failure to manually open IRWST squib valves during shutdown conditions with the RNS unavailable
10	IWN-MAN00C	Conditional probability of IWN-MAN00
11	LPM-MAN01	Failure to recognise the need for RCS depressurisation during a small LOCA or loss of high-pressure heat removal system
12	LPM-MAN-05	Failure to recognize the need for RCS depressurisation during a shutdown condition with failure of CMT and the RNS
13	OPA-1	Operator fails to deactivate the Protection and Safety Monitoring System (PMS) division involved in a fire
14	PDS6-MANADS	Failure to perform ADS as recovery from failure of automatic actuation in later phases of SGTR event.
15	REC-MANDAS	Failure to detect the need to perform an activity using the cues provided by diverse actuation system, or the probability to perform an activity by using the controls that are DAS related.
16	RECMANDAS	Conditional probability of REC-MANADS
17	REN-MAN03	Failure to recognise the need and failure to open recirculation valves to flood reactor cavity after core damage
18	REN-MAN04	Failure to recognise the need and failure to open the recirculation valves during a loss-of-coolant accident or transient, if the IRWST low-level signal fails – preventing automatic actuation of sump recirculation
19	RHN-MAN04	Failure to recognise the need and failure to isolate the RNS system, given rupture of RNS piping when the plant is at hot/cold conditions
20	RHN-MAN05	Failure to recognise the need and failure to initiate gravity injection via RNS hot leg connection during shutdown events
21	VLN-MAN01	Failure to recognise the need and failure to actuate the hydrogen control system, given core damage following a LOCA

34 This minimum set of post-fault actions has been included in the PSA HRA, which we have assessed and have judged the Westinghouse calculated human error probabilities (HEPs) to be potentially optimistic. The HRA calculations rely heavily on assumptions (both explicit and implicit) about the human system interfaces and operator cues, the procedures, and the control room operating regime. Our HRA assessment also notes that some of the cited HEPs are likely to be more difficult to substantiate and/or will require an amendment of the HRA.

35 The main explicit assumptions used in the HRA are described in Section 30.4 of Ref. 11. These relate to the following:

- Diagnosis modelling.
- Initiation of operator actions.
- Dependency.
- Operator stress level.
- Control room indications.
- Recovery.
- Time scales.

The validity of the assumptions will be assessed in detail during GDA Step 4.

36 The modelled HFEs have been analysed in the main at-power Level 1 PSA to determine their risk contribution and importance. Key results include:

- Table 50.7 of Ref. 11 shows 10 HFEs with a Risk Reduction Worth >1.
- Table 50.8 of Ref. 11 shows 7 HFEs with a Risk Achievement Worth > 2.
- Section 50.4.3 of Ref. 11 shows that a sensitivity study putting 30 modelled post-fault operator actions (relating to safety systems) to 0.0 only gives slightly smaller CDF – indicating that making these actions perfect gives little risk reduction.
- Section 50.4.3 of Ref. 11 shows that a sensitivity study setting 30 operator actions to fail (HEP = 1.0) [those relating to safety systems] increases the CDF to 1.4×10^{-5} pr year (from 2.41×10^{-7}) i.e. a 58-fold increase. This indicates that ensuring that those particular operator actions meet their assessed levels of reliability is an important contributor to reducing risk.

37 It is important to recognise that the human actions currently modelled in the Level 1 PSA are not the totality of human actions required to achieve safety on the AP1000. Hence, although our work on the PSA has provided some transparency on the human contribution to safety, it is not a complete model.

38 The shutdown and Level 2 PSA models have considered post-fault operator actions:

- Chapter 19.59-21 of the DCD states that *"human errors for shutdown faults are not overly important to shutdown CDF frequency. There is no particular dominant contributor. Sensitivity results show that the shutdown CDF frequency would remain very low even with little credit for operator actions."* This only considers post-fault operator action claims and does not appear to consider the potential HFE contribution to shutdown initiating events or indeed any pre-initiating fault HFE.
- For the Level 2 at-power PSA the large release frequency (LRF) is sensitive to the operator action to flood the reactor cavity in a short time following core damage. This will be assessed in detail during Step 4.

39 There are further referenced documents that contain information that would help to generate and support the position on required human actions for the AP1000. These

have not been formally assessed for GDA Step 3 but will form the basis of my assessment for GDA Step 4, and are listed below. It should be noted that those documents which are not yet formally approved documents within the Westinghouse Quality Management System (those with alphabetic revision numbers) will require to be formally issued to allow my assessment.

- WCAP-14644-NP R1 describes the allocation of function for the control room operators for AP-600/1000, and provides details of the Critical Safety Functions (CSFs) that the operator is expected to monitor post-fault via Emergency Procedures.
- APP-OCS-GJR-002, Rev. A describes the Concept of Operations and includes the relationships between the reactor operator, senior reactor operator and senior technical advisor. It provides an overview of the use of procedures and the basic workstation functions.
- APP-GW-GLR-010.doc-6/12/07 provides further details on the allocation of roles and responsibilities.
- APP-GW-GL-011 March 2006: *AP1000 Identification of Critical Human Actions and Risk Important Tasks*. This key document provides an analysis of the modelled critical and risk important human actions.
- APP-OCS-J1R-120 Rev. 0 December 2006: *AP1000 Operational Sequence Analysis (OSA-1) Summary Report*. This document summarises the OSA and uses APP-GW-GL-011 to consider key human actions/errors in key sequences.
- APP-OCS-J1R-120 Rev. A May 2009: *AP1000 Operational Sequence Analysis (OSA-2) Summary Report***.** This document provides the results of the Operational Sequence Analysis (OSA-2) of the AP1000. It summarises the OSA-2 results of nineteen risk-important tasks and three tasks that were identified as having potential human performance concerns. The analysis addresses the completeness of information, time to perform tasks, operator workload and operational crew staffing. It also summarises analyses of fourteen maintenance, test, inspection and surveillance tasks that have been identified as being 'risk-important'. However it should be noted that this analysis focuses on the operational requirements of the task rather than the human error potential.

40 I raised Regulatory Observation (RO) RO-AP1000-37 (Ref. 13) which placed an action on Westinghouse to *"provide documentation that clearly defines and justifies the role of human safety actions on AP1000…….this should encompass all aspects of human involvement on a proportionate basis…."*. To date this RO has not been addressed satisfactorily. The current position is that Westinghouse has provided a fully resourced programme that shows delivery of a compete safety case for HF at the end of February 2010; this will permit my detailed assessment during GDA Step 4.

41 It should be noted that if the safety case for HF is delayed, then it is likely that this matter will progress to a Regulatory Issue.

2.3.3.1 Availability and Age of Supporting Analysis (Substantiation/Analysis of the Human Based Safety Claims)

42 This aspect of my assessment is supported by my consideration of the human factors integration to the AP1000 (Section 2.3.5 of this report refers). The aim of this aspect of my assessment is to determine whether the scope of HF analyses is available to underpin/substantiate the human based safety claims, for assessment during GDA Step 4 (i.e. the 'evidence' base).

43 It is clear from the reference listing in the relevant PCSR extracts and Chapter 18 of the DCD that there is a significant volume of detailed HF analyses available. The scope of

these analyses appears to be consistent with what I would expect to support a design project of this type and size.

44 However there is no HF safety case/documentation that provides a safety context for the HF analyses, and which links the evidence base to the safety claims and arguments, as I would expect.

45 In terms of the age of analyses, I note that the HRA was undertaken for the AP600 design (mid 1990s). This may not be of concern if the assumptions base of the AP600 HRA analyses has been subsequently substantiated against the AP1000 operating regime.

2.3.4 Appropriateness of Standards Applied

46 The reference base of the DCD Chapter 18 has been reviewed to determine whether the standards that have been applied to the HF work are current. This is important from an ALARP perspective (refer to para. 19 of this assessment report), and the detailed output of the review is presented in Table 2 of this report.

47 In summary it appears that the majority of standards / references used have been superseded, and were current around the time of the AP600 certification. Although for some areas this is of no concern (where the standard/reference relates to 'first principles' / basic HF methods for example), in other areas it is of concern, particularly for example where this relates to control and display technology, which has increased in capability, flexibility and complexity over time.

48 As a result I raised Technical Query (TQ) TQ-AP1000-173 (Ref. 14) requesting that Westinghouse *"provide a benchmark of the methods and standards used against best practice and modern standards, across all aspects of the human factors work. Where HF analysis and design input has applied standards and methods that have subsequently been superseded, Westinghouse should either update the relevant analysis or justify why the use of older standards and methods remains"*.

49 The Westinghouse reply to TQ-AP1000-173 (Ref. 14) states that "*The AP1000 human factors program has applied the latest available approved standards regarding methods and design guidelines"* (and provides a documented list). It further states that *"if any new methods or standards are developed or superseded, then Westinghouse will address this on a case-by-case basis….."*. I do not consider this response acceptable, in that it does not provide the benchmark / gap analysis that the TQ requests. This will be taken forward during GDA Step 4.

2.3.5 Human Factors Integration (HFI)

50 This aspect of my assessment was undertaken in accordance with the TAG on HFI, which states that:

- *"Human factors integration (HFI) is a good practice approach to the application of human factors to systems development. As a methodology it provides an organising framework to help ensure that all relevant HF issues are identified and addressed. In addition the HFI approach has a management strategy that aims for timely and appropriate integration of human factors activities throughout the project.*
- *'Integration' means "…a combination of parts …that work well together..". Therefore HFI requires that HF is an integral part of a project, and is not carried out in isolation.*
- *The level of HF integration should be commensurate to the size of the project, and take account of the safety reliance on humans and the consequences of human error, together with the novelty and complexity of any new technology"*.

51 This aspect of my assessment therefore focused on the range of activities undertaken by the Westinghouse HF engineering programme, with some consideration of the use of Suitably Qualified and Experienced Personnel (SQEP), where possible. This would provide me with a level of confidence that the type of analysis I would expect for a project of this size is available, and is likely to be of a suitable quality.

52 There is a large body of material available that cites the HF work undertaken to date; the majority of which appears relevant and will facilitate HFI. Chapter 18 of the DCD cites the scope of work for the HF engineering programme and this appears to cover the scope of HF technical areas that I would expect to see, with the exception of human reliability (which is referenced out to the PSA).

53 Of merit is the functional analysis, which appears thorough, the wide ranging task analytical work (including workload analysis) and the extensive evidence of the human system interface work undertaken by Westinghouse. It should be noted that this work has not been assessed, but its availability provides a level of confidence that the 'evidence' base to support a safety case for HF is in place.

54 Chapter 18 of the DCD also provides job specification criteria for HF personnel. This provides confidence that the matter of SQEP resource is recognised and being applied to the AP1000 design.

55 However at this stage of my assessment it appears that there may be a knowledge/assessment gap in terms of administrative controls. It appears that Westinghouse is limiting this to their Technical Specifications, which although a critical aspect of the administrative controls system, is not the totality.

56 In addition it appears that while the scope of the HF engineering work facilitates HFI input to the NPP design, what is less clear is the HFI input to the development of the safety documentation.

57 I therefore raised Technical Query TQ-AP1000-172 (Ref. 14) requesting that Westinghouse *"provide a description of the HFI to the AP1000 design development and safety documentation development…".* Westinghouse have provided a response to this TQ by citing major references that map onto the process flow diagram cited in the ND TAG on HFI [Draft]. This response has not been assessed since it was received at the end of GDA Step 3, and I will continue to probe the HFI during GDA Step 4.

2.3.6 Additional Assessment Area – Novel Technology

58 It is important to identify the application of new or novel technology that may present HF issues that have not been considered previously in the UK. Should this be the case, I may have to undertake research to determine current and best practice, to enable me to form a regulatory judgement. In addition for GDA Step 4 I would ensure that Westinghouse has fully analysed and understood the potential human reliability issues relating to such technologies.

59 The PCSR notes the evolution of the AP600 design, but makes little reference to any specific technology advances that might affect the Human System Interface (HSI) and other HF aspects. The DCD notes in Section 18.2 that technology has advanced, but places an emphasis on the use of proven, reliable technology (without clarifying the manner in which it is considered proven).

60 Section 18.8 of the DCD describes the HSI design. A number of aspects of the design are noted where it can be considered that new technology is a significant element of the design philosophy:

- Use of computerised procedures. There is a clear intention to use such an approach and the DCD notes that any proposed use will be subject to suitable validation and

verification, but without elaborating on the manner in which this will be undertaken. Although not currently in use in the UK, there is a considerable body of research available in this area to inform regulatory assessment. I also note the potential issue of ensuring independence of the computerised procedure system from the PMS, and will liaise with our control and instrumentation (C&I) assessor on this matter.

- The use of soft controls is planned. Although this is not a common feature of existing UK NPPs it is no longer appropriate to consider this 'new technology' given its widespread use throughout process control. A programme to validate the intended Human System Interface (HIS) design is proposed by Westinghouse.
- The alarm system and safety parameter display system can be considered as deploying existing technology. However, given their significance, and the use of flexible methods of information presentation, there is an appropriate focus on the process for designing and validating the proposed implementation. The information hierarchies also are not 'new technology' in the strict sense, but represent potentially novel ways of structuring and representing plant information.
- The use of automated devices and robotics is being considered by Westinghouse in the context of design for maintainability. The significance of this is noted, but no information is provided concerning the issues, the extent of the proposed use, or the manner in which it will be designed and validated.
- A wireless communications system is proposed. Although this introduces HF issues, it is reasonably well-established technology.

61 In summary, the AP1000 does not include the use of significant novel or unproven technology that would present unfamiliar HF issues and thus generate a research requirement to inform our GDA Step 4 assessment.

2.3.7 International Regulators' Assessments

62 The Multi-national Design Evaluation Programme (MDEP) has recently convened a grouping of experts on HF and held its inaugural meeting. I am representing the UK on this forum, which will provide an opportunity for information exchange on regulatory assessment, including that for the AP1000 design. In addition I am committed to visiting the US NRC and CNSC in December 2009 to exchange technical assessment information relating to the HF aspects of the AP1000. This meets our desire and commitment to be cognisant of international regulators' assessments of the reactor designs seeking a generic design certificate in the UK.

63 I have briefly considered the US NRC assessment. I note that NRC staff have reviewed Chapter 18 of the DCD, principally using assessment criteria cited in NUREG-0711 (Ref. 7), NUREG-0800 (Ref. 15), NUREG-0700 (Ref. 16) and US Regulatory Requirements 10CFR50.34(f), 10CFR50.34(g) (Ref. 17) and 10CFR52.47 (Ref. 18). They have undertaken the HRA methodological aspects separately (via the PSA assessment) to the HF engineering assessment, and for this stage of my assessment I am not clear what, if any, benefit I can take from the NRC approach to the HF assessment. Principally this is a result of the prescriptive regulatory regime in the US, specifically that there is not a requirement to present a safety case that clearly identifies safety claims, arguments and evidence.

2.3.8 Research Requirements

64 Ref. 9 highlights that the AP1000 HRA uses the Technique for Human Error Rate Prediction (THERP) (Ref. 19) data. However, the AP1000 design, particularly for all control room post-fault actions, uses interfaces that are very different to those assumed in

the THERP data sets. ND needs to form a view on the work that would be necessary to evaluate THERP data against digital interfaces and whether additional research work is required.

2.3.9 Potential Exclusions

65 There is the potential for the complete HF technical area to be an Exclusion to the GDA process in the event that we do not receive an adequate safety case for HF early in GDA Step 4.

3 CONCLUSIONS AND RECOMMENDATIONS

66 Westinghouse has not presented a UK safety case for HF. The PCSR extracts and DCD Chapter 18 provide an overview of their programme and processes, but there is no claims, arguments, evidence structure to the HF documentation.

67 There is no complete citation of the totality of human based safety claims, although there is a listing with associated analysis of some post fault operator actions. What appears to be lacking is an explicit consideration of the following (also raised in our assessment of the HRA for the PSA technical area):

- The impact of maintenance type human errors (including testing, inspections and surveillance).
- The potential impact of post fault human errors that could degrade or disable key passive safety systems (as a result of fault mis-diagnosis).

68 There does appear to be the type of detailed HF analyses that I would expect. However this is at the 'arguments' and 'evidence' level and it is difficult for me to understand the safety relevance and contribution without a clear linkage to the safety claims on human actions.

69 There is an issue with regard to the age of the standards applied to the design, and I expect a benchmarking exercise to be undertaken to demonstrate the acceptability of the standards used when compared to modern standards.

70 Westinghouse has committed to providing a UK style safety case for human factors, which links the HF analyses to the safety contribution of human actions (Ref. 20). This is programmed for delivery early in GDA Step 4.

71 I have received a fully resourced and detailed programme from Westinghouse showing the route to delivery of the safety case for HF. This provides a level of confidence in their ability to meet the March 2010 deadline.

72 On the basis of their commitment to the development of the HF safety case, and the programme presented, I am able to recommend progression of the Westinghouse AP1000 to GDA Step 4 in the technical area of HF.

73 However it should be noted that if the HF safety case be delayed, or judged to be insufficient to facilitate a meaningful GDA Step 4 assessment in the area of HF, it is likely that a Regulatory Issue will be raised.

4 REFERENCES

1 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732, Revision 1, Westinghouse Electric Company LLC, March 2009.

2 *ND BMS, Assessment Process.* AST/001, Issue 2, HSE, February 2003.

3 *ND BMS, Guide: Assessment Process.* G/AST/001, Issue 2, HSE, February 2003.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition, Revision 1, HSE, January 2008.

5 *Generic Design Assessment – New Civil Reactor Build. Project Initiation Document for Step 2/3 Human Factors Assessment.* ND Division 6 Assessment Report AR 09/007. July 2009. TRIM Ref. 2009 / 281513.

6 *AP1000 European Design Control Document.* EPS-GW-GL-700, Revision 0, Westinghouse Electric Company LLC, February 2009

7 *Human Factors Engineering Review Model.* NUREG-0711, Rev. 1, US Nuclear Regulatory Commission. May 2002.

8 *Reactor Safety Reference Levels* Issue O Western European Nuclear Regulators Association (WENRA) January 2008.

9 . *ND BMS Technical Assessment Guides:*

- *ND Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable).* T/AST/005, Issue 4 Rev. 1. HSE. January 2009.
- *Early Initiation of Safety Systems.* T/AST/010. Issue 2. HSE. July 2008.

10 *Generic Design Assessment – New Civil Reactor Build. Step 3 Probabilistic Safety Analysis of the Westinghouse AP1000.* ND Division 6 Assessment Report AR 09/017. November 2009. TRIM Ref. 2009 / 335823

11 *UK AP1000 Probabilistic Risk Assessment*. UKP-GW-GL-022, Revision 0, Westinghouse Electric Company LLC, May 2007

12 *AP1000 Operational Sequence Analysis (OSA-1) Summary report.* APP-OCS-J1R-120, Revision 0, Westinghouse Electric Company LLC, December 2006

13 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 3.* HSE-ND, TRIM Ref. 2009/358257.

14 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 3.* HSE-ND, TRIM Ref. 2009/358248.

15 *Standard Review Plan.* NUREG-0800, US Nuclear Regulatory Commission. 1996.

16 *Human-System Interface Design Review Guideline.* NUREG-0700, Rev. 2, US Nuclear Regulatory Commission. May 2002.

17 US Nuclear Regulatory Commission Regulations: *Title 10, Code of Federal Regulations, Part 50, Domestic licensing of production and utilization facilities*.

18 US Nuclear Regulatory Commission Regulations: *Title 10, Code of Federal Regulations, Part 52*, *Licenses, certifications, and approvals for nuclear power plants*.

19 *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* NUREG/CR-1278, Swain, A. D., & Guttman, H. E. (1983).

20 *Westinghouse letter – Human Factors.* Westinghouse Electric Company LLC UN REG WEC 000097, 2 October 2009. TRIM Ref. 2009/394331.

Table 2

Detailed Assessment of Human Factors Related Standards Cited in the European DCD

DCD Ref.	Text / Title	Assessment Comment
18.1.1	NUREG-0711, Human Factors Engineering Program Review Model, U.S. NRC, July 1994.	Now at Revision 2. This reference is considerably out of date.
Fig 18.1.1		This figure omits several elements of HFE, for example environmental design and job design.
18.2.1.1.	The goal of the human factors engineering program is to provide the users of the plant operation and control centers effective means for acquiring and understanding plant data and executing actions to control the plant's processes and equipment. The objective is to enable personnel tasks to be accomplished within time and performance criteria.	The HFE programme goal is severely limited to just HMI / HCI topics. Later the goal is expanded to suggest that additional areas might be covered, but the evidence is scant and not supported by the standards that will be used to ensure good practice is followed.
18.2.1.3	Facilities included in the scope of the AP1000 human factors engineering program are the main control room (MCR), the technical support center (TSC), the remote shutdown room, the emergency operations facility (EOF), and local control stations.	As above.
18.2.3.1	Documents produced as part of the instrumentation and control and human system interface design process include: • Operating experience review documents • Task analysis documents • Functional requirements documents • Human system interface design guidelines documents • Design specification documents • Instrumentation and control architecture diagrams • Block diagrams • Room layout diagrams • Instrumentation lists • System specification documents	There is no mention of producing a Target Audience Description (TAD) document. For a plant designed to domestic codes and standards, a TAD document is essential for the target market to ensure that national stereotypes do not result incompatibility issues.
18.2.7	Reason, J. T., "Human Error," Cambridge, U.K., Cambridge University Press, 1990.	Although still considered to be a useful text on the topic, later publications on the topic do exist which expand upon the body of knowledge on the topic of Human Error. For example, Reason published on the specific topic of Human Error in Maintenance in 2003.

DCD Ref.	Text / Title	Assessment Comment
18.4.2	NUREG/CR-3331, "A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control," 1983.	Technology has considerably advanced in its ability to take on roles that were traditionally allocated to the operator. Standard IEC 61508 also has a considerable impact on allocation of function studies.
18.5.5.	U.S. NRC Guidance, NUREG/CR-3371, "Task Analysis of Nuclear Power Plant Control Room Crews.	This report was published in 1984 when technology like computer based procedures and SCADA type systems were not used within nuclear control rooms. Is this now appropriate for a modern plant design which will feature both types of system?
18.5.5	IEC-964, "Design for Control Rooms of Nuclear Power Plants."	It does not state which version was used, but more recent standards such as : IEC 60964 IEC 60965 IEC 61772 IEC 61227 should be considered as well
18.5.5	Woods, D. D., "Application of Safety Parameter Display Evaluation Project to Design of Westinghouse SPDS," Appendix E to "Emergency Response Facilities Design and V & V Process," WCAP-10170, submitted to the U.S. Nuclear Regulatory Commission in support of their review of the Westinghouse Generic Safety Parameter Display System (Non-Proprietary) (Pittsburgh, PA, Westinghouse Electric Corp.), April 1982.	This document was published in 1984. The technology used for presenting Safety Parameters in 1984 has totally changed so this reference could be no longer applicable.
18.6.2	Combined License applicants referencing the AP1000 design will address the staffing levels and qualifications of plant personnel including operations, maintenance, engineering, instrumentation and control technicians, radiological protection technicians, security, and chemists. The number of operators needed to directly monitor and control the plant from the main control room, including the staffing requirements of 10CFR50.54(m), will be addressed.	This statement is weak and offers no evidence for how this will be achieved. It even suggests that the licensee will be required to justify manning levels. For the HMI to effective, the proposed manning level needs to be known. This should be an outcome of the task analysis and allocation of function studies. Later in Section 18.8.3.2 the report does state that Reference 44 “WCAP-14694, “Designer’s Input to Determination of the AP600 Main Control Room Staffing Level,” Revision 0, July 1996.” provides input to the staffing levels

DCD Ref.	Text / Title	Assessment Comment
18.8	The wall panel information system presents information about the plant for use by the operators…it provides information important to maintaining the situation awareness of the crew and for supporting crew coordination…The wall panel information system is a non safety-related system. It is designed to have a high level of reliability. The plant information system…these displays provide information important to monitoring, planning, and controlling the operation of plant systems and obtaining feedback on control actions. The displays provided by the plant information system are non safety-related displays, but provide information on both safety-related and non safety related systems.	Consider this issue in GDA Step 4: the acceptability of classing a display system as non safety related and yet presenting information to the operator on it that could be classed as safety related.
18.8.1.1	The operations and control centers functional requirements document includes requirements to meet failure, diversity, electrical separation, and other applicable criteria. This document establishes requirements related to access control, redundancy, independence, identification and test capability, and defines requirements on system inputs and outputs.	There is no indication as to how Westinghouse proposes to balance the conflicts of segregation, diversity, and redundancy with human factors needs. For example, are manual valves located together for operability reasons or segregated for survivability reasons.
18.8.1.1	Reference 25 describes the operator decision-making model and associated operator cognitive activities. As shown in Figure 18.8-2, the HSI interface resources are mapped to four major classes of operator cognitive activities in the model (detection and monitoring, interpretation, control, and feedback).	Considerable research has been done in the area of supporting Tactical and Strategic decision making. This is particularly important when switching from normal operations to accident management. The model shown in 18.8-2 makes no reference to the difference between strategic / tactical decision making.
18.8.1.5	Mock-Up activities	The report discusses the use of passive prototyping to obtain feedback on the operability of design.
18.8.1.9	Environmental Design Standards Beranek, L. L., “Revised Criteria for Noise in Buildings,” Noise Control, Vol. 3, Nr.1, p. 19ff. Grandjean, E., “Fitting the Task to the Man: An Ergonomic Approach,” London: Taylor and Francis Ltd., 1981. Van Cott and Kinkade, “Human Engineering Guide to Equipment Design,” Washington D.C.: U.S. Government Printing Office, 1972.	The report claims that well accepted standards are used to define environmental conditions pertinent to the control room areas. The standards quoted are 20-30 years old. Considerable research on environmental ergonomics has been done since the publication of the listed standards.

DCD Ref.	Text / Title	Assessment Comment
18.8.2.2	Display of Safety Parameters	The report makes no mention of warnings and does not reference a formal alarms and warning philosophy as would be expected.
18.8.3.2	Each reactor operator workstation contains the displays and controls to start up the plant, maneuver the plant, and shut down the plant.	There are known supervision and control of operations issues with the ability to control the plant from multiple workstations. The report makes no mention of these issues or how they will be controlled.
18.8.3.2	The supervisor workstation is identical to the reactor operator workstations, except that its controls are locked-out. The supervisor workstation contains both internal plant and external plant communication systems.	There is evidence to suggest that supervisor stations should be designed specifically for supervision and not just as a duplicate of operator stations.
18.8.4	Human Factors Design for the Non-Human-System Interface Portion of the Plant	There are no references supporting the design of the non HSI sections of the plant section. The emphasis in this report is very much on the HMI / HCI within control rooms and local to plant stations. Although HF issues of wider plant context are briefly mentioned, there is insufficient information to form a view of their adequacy.
18.8.6	CEI/IEC 964, “Design for Control Rooms of Nuclear Power Plants,” International Electrotechnical Commission, Geneva, Switzerland, 1989.	Later standards exist.
18.8.6	IEEE Std 1289-1998, “IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.”	Later standards exist.
18.8.6	MIL-STD-1472, Department of Defense Design Criteria Standard: Human Engineering, Revision F, August 1999.	Later standard – revision F – exists.
18.8.6	NUREG/CR-6634, “Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance,” U.S. Nuclear Regulatory Commission, Washington, D.C., March 2000	Later standards exist.
18.8.6	For brevity the other standards are not listed as they total a further 47; the majority of which are superseded by research and later standards.	

DCD Ref.	Text / Title	Assessment Comment
18.10.2	WCAP-14655, "Designer's Input to the Training of the Human Factors Engineering Verification and Validation Personnel," Revision 1, August 1996.	Later standards exist.

Annex 1 – Human Factors – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None.				
Regulatory Observations				
RO-AP1000-37	10 July 2009	Westinghouse has not been able to provide a statement of the HF philosophy, the role of human action (in terms of safety contribution) and the concept of operation for the AP1000, or point to the relevant documentation where such information is presented. The material presented in the inaugural meeting 17-18 June 2009 was at a detailed design level and largely relevant to the control room design. Westinghouse was not able to frame this detail into a safety context to facilitate ND understanding of the relative risk contribution from human actions.	Unresolved. Westinghouse have provided a commitment and programme to deliver a UK safety case for HF at the beginning of March 2010.	GDA Step - by March 2010