New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-HF-01 Completeness of the Human Factors Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential.

Assessment Report: ONR-NR-AR-16-021-AP1000
Revision 1
March 2017

Published 03/17

EXECUTIVE SUMMARY

The purpose of the Generic Design Assessment (GDA) process is to determine whether a reactor design is capable of being built and operated in Great Britain (GB), on a site bounded by a generic site envelope, in a way that is acceptably safe and secure. A Design Acceptance Confirmation (DAC) is issued when the Office for Nuclear Regulation (ONR) and the Environment Agency (EA) are confident that sufficient information has been provided and that no significant safety, environmental or security issues have been identified that cannot be resolved.

Westinghouse Electric Company (Westinghouse) is the reactor design company for the **AP1000®** reactor. Westinghouse completed (GDA) Step 4 in 2011 and then paused the regulatory process. At that point, it achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to award of a DAC and before any nuclear safety related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report relates to the ONR's assessment of the Westinghouse **AP1000®** reactor design in the area of Human Factors (HF). This report addresses GDA Issue GI-AP1000-HF-01.A1 which encompasses a number of Step 4 Regulatory Observations relating to limitations in Human Error Analysis (HEA). The issue concerns the - **Completeness of the HF Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential**.

Before Westinghouse paused the **AP1000®** GDA it attempted to close this issue by submitting a significant volume of HF analysis towards the end of GDA Step 4. This analysis related to human error mechanisms, operator misdiagnosis and violation potential but was outside ONR's assessment window. ONR undertook an initial high-level review of the submission to gain confidence in the approach but was unable to undertake a sufficiently detailed and thorough assessment within the Step 4 timescales to arrive at a formal regulatory judgement. GDA issue GI-AP1000-HF-01.A1 was raised to capture the ongoing requirement to consider human error and to ensure appropriate consideration moving forward.

Following Westinghouse's re-engagement with the GDA process, my preliminary assessment of the analysis submitted late in Step 4 identified that it was not sufficient to meet regulatory expectations in relation to human error analyses and to close the issue. This was because the analysis lacked depth with respect to substantiating and analysing Human Based Safety Claims (HBSCs) and revealed limitations in Westinghouse's Human Factors Integration (HFI) process with respect to the scope of HF influence across the project and the resulting impact on HBSCs.

To address these limitations, Westinghouse developed a GDA Issue Resolution Plan which presented its approach for closing GI-AP1000-HF-01. Key elements of this include:

- performing a systematic assessment of HF integration across the remaining 50 GDA issues;
- performing an HF review of approved selected **AP1000®** Design Change Proposals (DCPs) to identify any human actions created as part of the design changes approved by Westinghouse since the Reference Date of 16 September 2010;
- assuring human error identification completeness and assessing the potential use of optimistic claims through:
    - review, and revision as required, of existing AP1000 Human Factors Safety Case supplemental documents to UKP-GW-GL-042, revision 0; and
    - use of a sampling plan approach for the review of claims on operator actions; substantiating the claims where possible and identifying assumptions - where

substantiation of claims is not possible, qualitative reassessment of the action consequences;

- incorporating assessment, results, and findings from these efforts into subsequent revisions to the **AP1000®** Pre-Construction Safety Report, UKP-GW-GL-793.

My assessment has included review of the outputs from each of these activities supported by consideration of additional evidence from Westinghouse's wider design and safety case analyses. In undertaking my assessment I have focused on three main areas of consideration. These are:

- HFI: with a view to confirming the completeness of the HF Safety Case and HBSCs included for assessment as part of this issue.

- HEA: with a view to ensuring the adequacy of the qualitative substantiation of important operator actions and the appropriate treatment of error mechanisms, misdiagnosis and violation potential; and

- sensitivity of the design and safety analyses to the HBSCs: with a view to better understanding the risk importance of the HBSCs and ensuring a proportionate approach to their assessment.

My principal findings in these areas are:

Human Factors Integration

In general I have found that Westinghouse applied itself to the integration of HF and that its processes now adequately support the identification and analysis of HBSCs. In particular, I note that Westinghouse expanded its scope of identification by assessing all 51 GDA issues for additional previously unidentified HBSCs. Westinghouse also proportionally reviewed all DCPs and identified additional previously unidentified HBSCs. This gives confidence in the rigour and completeness of the HBSC identification process.

I found that HBSCs are managed via Westinghouse's Human Action Database and I am content with Westinghouse's method for selecting HBSCs from the database for further detailed analysis and substantiation. I have reviewed the method and underpinning criteria and judge that they combine risk and representation to inform the selection of HBSCs. I consider this to be a sensible and proportionate approach.

In addressing this issue, I note that Westinghouse responded constructively to challenges made by ONR and has put considerable time and effort into the development of its expertise in this area. As a result of this, it is my view that Westinghouse has developed a credible and responsive HF design and analysis capability. This is important in supporting the effective deployment of HFI, the reliable identification of HBSCs, and ultimately in supporting the licensing of the **AP1000®** design.

Human Error Analysis

From my review of Westinghouse's HEA, it is clear that there has been a number of challenges in the development of a cogent and coherent suite of analyses through which to present its findings for the **AP1000®** design. Westinghouse has, however, persevered in applying itself to the issues raised and in doing so, has ultimately brought together a strong set of supporting evidence, as detailed below:

Westinghouse initially submitted a significant quantity of paper-based HEA which, while having some value, did not sufficiently meet regulatory expectations with regard to the scope and depth of analysis. This analysis did, however, provide a valuable basis for discussion, including consideration of misdiagnosis and the potential for violations. From this dialogue, Westinghouse built on and extended its original analysis to develop a revised iteration of the paper based human error method. I have reviewed this approach and consider it to be consistent with GB best practice. I note that the analysis performed using this method, while

currently limited in its extent of application, provides confidence that future HEA work undertaken to address the extant Step 4 assessment findings will be of good quality. I further note and welcome that Westinghouse has committed to updating or re-assessing existing analysis using this new analysis method and that these human error analyses will be provided as input into the probabilistic safety analyses during site licensing.

In addition to the paper-based analyses, Westinghouse has also presented credible evidence relating to the substantiation of operator actions from its Integrated System Validation (ISV) trials. These have comprised a thorough analysis of the human system performance of the Main Control Room (MCR) and the Remote Shut-down Room (RSR). This analysis addresses the majority of HBSCs associated with normal operations and faults that contribute to core damage. I have found that the trials provided a valuable opportunity to evaluate the HBSCs and to scrutinise associated errors and that, in effect, the range and depth of analysis undertaken by Westinghouse substantiates the majority of HBSCs. In addition, where HBSCs have not been substantiated through the trials, the root causes have been identified and solutions are currently being progressed. Westinghouse has also committed to verifying and validating these solutions during further planned trials. I consider this to be strong supporting evidence in relation to the substantiation of HBSCs, and note that the trials have also promoted holistic consideration of both diagnostic error and the potential for violation.

In addition to the submission provided by Westinghouse, I have observed a number of scenarios which contain HBSCs in the **AP1000®** MCR simulator. From my observations I consider that the Control & Instrumentation (C&I) is well laid out, presenting clear and unambiguous information to the operators. Noting the artificiality of a simulation, the crew were reliably able to detect and diagnose plant faults and respond in a timely manner. Intra-crew communications reflected relevant good practice and the crew demonstrated a high level of shared situational awareness. I further note that the conduct of operations worked well as did the procedures.

Risk sensitivity of the design and safety analyses to the HBSCs

My assessment found that the **AP1000®** design places only limited reliance on the HBSCs to remain within target safety limits. In particular I note that the extant at-power Probabilistic Safety Analysis (PSA) shows that if all HBSCs fail (human error probabilities are set to 1.0), the core damage frequency increases by a factor of100 and moves to 1.8E-05/year. When credit for containment is considered at 0.1/demand this is well within the ONR Target 8 Base Safety Limit (BSL) of 1E-4/year and gives confidence that safety targets will be achieved. (Target 8 is for an off-site dose greater than 1000 mSv).

With credit for containment the frequency of an off-site dose greater than 1000mSv is around the Base Safety Objective (BSO) of 1E-6/year. While taking no credit for human actions within the PSA is sensitive, based on Westinghouse's analysis, I judge that ONR BSLs can be met and risks below BSOs would be expected once containment is considered and realistic human failure rates are used within the probabilistic risk model.

While my expectation is that Westinghouse will develop a complete and credible HF Safety Case, with adequate demonstration of the safety claims and requirements on the human actions this analysis gives confidence that the **AP1000®** design is relatively insensitive to degradation in performance of the HBSCs.

Conclusions

Overall, Westinghouse has undertaken a significant volume of Human Factors assessment in addressing this GDA issue and has applied considerable competent HF resource. I note in particular the strength and depth of evidence to substantiate the HBSCs provided by Westinghouse's ISV trials, and the recent iteration of its paper-based human error method which I consider to be consistent with GB best practice.

Based on review of this evidence, it is my view that Westinghouse's submissions, when viewed holistically, identify, analyse and substantiate* the key HBSCs so far as is reasonably practicable for GDA. I further note that Westinghouse has provided compelling holistic evidence supported by a reasonable set of assumptions that both diagnostic errors and the potential for violation can be reduced to As Low As Reasonably Practicable (ALARP) on the **AP1000®** design.

While a number of minor issue remain which should be taken forward as part of the site specific safety submissions, I have identified no sufficiently significant safety issues in the area of HF that could prejudice the closure of GI-AP1000-HF-01 or the issuing of a DAC.

* Where tasks have not been substantiated, a credible resolution process has been observed, providing confidence that the task can be substantiated as the design progresses

LIST OF ABBREVIATIONS

AC	Alternating Current
ADS	Automatic Depressurisation System
AF	Assessment Finding
ALARP	As Low As Reasonably Practicable
ATWS	Anticipated Transient Without Scram
BDBA	Beyond Design Basis Accident
BSL	Base Safety limit
BSO	Base Safety Objective
C&I	Control and Instrumentation
CCS	Containment Cooling System
CDF	Core Damage Frequency
CET	Core Exit Thermocouple
CMT	Core Make-Up Tank
COTS	Commercial Off-the-Shelf
CRM	Crew Resource Management
CSF	Critical Safety Functions
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DBA	Design Basis Accident
DC	Direct Current
DCP	Design Change Proposal
DDS	Data Display and Processing System
EA	Environment Agency
EOP	Emergency Operating Procedure
FRP	Functional Restoration Procedure
GB	Great Britain
GDA	Generic Design Assessment
HAD	Human Action Database
HBSC	Human Based Safety Claim
HEA	Human Error Analysis
HED	Human Engineering Deficiencies
HEP	Human Error Probability
HF	Human Factors
HFA	Human Factors Analysis
HFE	Human Factors Engineering
HFI	Human Factors Integration
HRA	Human Reliability Analysis

HSI	Human-System Interface
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
INPO	Institute of Nuclear Power Operations
IRWST	In-Containment Refuelling Water Storage Tank
ISV	Integrated Systems Validation
IVR	In-Vessel Retention
LOCA	Loss of Coolant Accident
LRF	Large Release Fraction
MCR	Main Control Room
MDEP	Multi-national Design Evaluation Programme
MSIV	Main Steam Isolating Valves
MTIS	Maintenance, Testing, Inspection, and Surveillance
OD	Outer Diameter
OECD-NEA	Organisation for Economic Co-operation and Development Nuclear Energy Agency
ONR	Office for Nuclear Regulation
OpEx	Operating Experience
ORP	Optimal Recovery Procedures
P&ID	Piping and Instrumentation Drawing
OPEX	Operational Experience
PCCS	Passive Containment Cooling System
PCCWST	Passive Containment Cooling Water Storage Tank
PCCAWST	Passive Containment Cooling Auxiliary Water Storage Tank
PCSR	Pre-construction Safety Report
PDSP	Primary Dedicated Safety Panel
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment / Analysis
PRHR	Passive Residual Heat Removal
PSA	Probabilistic Safety Analysis
PSF	Performance Shaping Factor
PRA	Probabilistic Risk Assessment
PWR	Pressurised Water Reactor
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RGP	Relevant Good Practice
RIHA	Risk Important Human Actions

RNS	Normal Residual Decay Heat Removal System
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
RRW	Risk Reduction Worth
RSR	Remote Shutdown Room
RRW	Risk Reduction Work
RV	Reactor Vessel
SAA	Severe Accident Analysis
SAMG	Severe Accident Management Guideline
SAPs	Safety Assessment Principles
SAT	Systematic Approach to Training
SBO	Station Blackout
SFAIRP	So Far As Is Reasonably Practicable
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SQEP	Suitably Qualified and Experienced Person
SSC	System, Structure (and) Component
STA	Shift Technical Advisor
TAG	Technical Assessment Guide
TMI	Three Mile Island
US NRC	United States (of America) Nuclear Regulatory Commission
VLS	Containment Hydrogen Control System
WPIS	Wide Panel Information System

TABLE OF CONTENTS

1 INTRODUCTION 11
1.1 Background 11
1.2 Scope 12
1.3 Method 12
2 ASSESSMENT STRATEGY 14
2.1 Pre-Construction Safety Report (PCSR) 14
2.2 Standards and Criteria 14
2.3 Use of Technical Support Contractors 16
2.4 Integration with Other Assessment Topics 16
2.5 Out-of-scope Items 17
3 REQUESTING PARTY'S SUBMISSIONS IN RESPECT OF ISSUE GI-AP1000-HF-01 18
3.1 Summary of Closure Strategy 18
3.2 Details of Westinghouse's Submission 18
3.3 Summary of the Safety Case 24
4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-HF-01 26
4.1 Scope of Assessment Undertaken 26
4.2 Assessment of Human Factors Integration 27
4.3 Assessment of Human Error Analysis 30
4.4 Vulnerability of the AP1000® PWR Design to Human Error 52
4.5 Assessment Findings 53
5 CONCLUSIONS 55
5.1 Human Factors Integration 55
5.2 Human Error Analysis 55
5.3 Risk Sensitivity of the Design and Safety Analyses to the HBSCs 56
5.4 Overall Conclusions 56
6 REFERENCES 57

Table(s)

Table 1: Key Safety Assessment Principles used during the assessment
Table 2: TAGs used as part of this assessment
Table 3: Out-of-scope items - addressed during licensing
Table 4: Risk Important Human Actions Tested During The ISV Trials
Table 5: Mapping of ISV scenarios to highest core damage contribution faults

Annex(es)

Annex 1: Screening Criteria for HBSC Sample and HBSC listing
Annex 2: SAPs Considered as Part of my Assessment
Annex 3: List of HBSCs contained within Westinghouse submissions
Annex 4: List of ISV Trial Scenarios
Annex 5: List of Step 4 Assessment Findings Which Have Informed My Assessment
Annex 6: Screenshots of Phase 2 HEA Pro-forma – UKP-GW-GL-126

1 INTRODUCTION

1.1 Background

1. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and then paused the regulatory process. Westinghouse achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to award of a DAC and before any nuclear safety related construction can begin on site.

2. One of the 51 GDA issues (GI-AP1000-HF-01) (Ref. 1) concerns the **completeness of the Human Factors Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential**. This issue was synthesised from a number of outstanding Regulatory Observations (ROs), which comprised the following:

   - RO-AP1000-037 Demonstration of the Safety Claims and Requirements on Human Actions
   - RO-AP1000-090 Human Error Mechanisms
   - RO-AP1000-096 Misdiagnosis
   - RO-AP1000-097 Violations

3. At the point when the regulatory process was paused, Westinghouse considered that it had addressed the issues contained within GI-AP1000-HF-01 on the basis of submission of a substantial body of work prior to the end of Step 4, but outside the Office for Nuclear Regulation's (ONR's) assessment window. ONR undertook an initial high level review of the submission to gain confidence in the approach, but was unable to undertake a sufficiently detailed and thorough assessment within the Step 4 timescales to arrive at a formal regulatory judgement. GDA issue GI-AP1000-HF-01.A1 was raised to capture the requirement for this and to ensure appropriate consideration moving forward.

4. Westinghouse recommenced the GDA of its **AP1000®** design in September 2014, with a series of topic-based presentations explaining resolution strategies for the closure of the GDA. For GDA issue GI-AP1000-HF-01, Westinghouse presented the view that there should be little need for any new analysis due to the material previously supplied in 2011. It also stated that there would be no need for any additional Human Factors (HF) work beyond that needed to close GDA Issue GI-AP1000-HF-01. At the time, I advised Westinghouse that this was not a realistic position as it was clear to me that this analysis included insufficient depth with regard to analysing and substantiating HBSCs. In addition, I noted that other GDA issues had an HF component to them, thus requiring some level of HF assessment to support closure. Westinghouse responded positively to this advice and revised its resolution plan accordingly, committing to adequate Human Factors Integration (HFI) across all of the GDA issues. The resolution plan is outlined in Section 3 with full detail provided in Ref 2.

5. This report is the ONR's assessment of the Westinghouse **AP1000®** reactor design in the area of Human Factors. Specifically, this report addresses GDA Issue GI-AP1000-HF-01 Completeness of the Human Factors Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential

6. The related GDA Step 4 report is published on our website (**http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-hf-onr-gda-ar-11-012-r-rev-0.pdf**), and this provides ONR's assessment underpinning the GDA issue. Further information on the GDA process in general is also available on our website (**http://www.onr.org.uk/new-reactors/index.htm**).

1.2 Scope

7. The purpose of the GDA process is to determine whether a reactor design is capable of being built and operated in Great Britain, on a site bounded by a generic site envelope, in a way that is acceptably safe and secure. A Design Acceptance Confirmation (DAC) is issued when the ONR and Environment Agency are confident that sufficient information has been provided, and that no significant safety, environmental, or security issues have been identified that cannot be resolved. In order to make this judgement, a fully resolved safety case is not required, nor does the design need to be complete.

8. The scope of my assessment considers the completeness of the HF Safety Case with specific reference to the three key limitations identified in GDA issue GI-AP1000-HF-01. These relate to:

- The efficacy of Westinghouse's analysis and substantiation of the HBSCs on the **AP1000®** reactor design.
- How well the **AP1000®** design supports reliable fault diagnosis; and
- Whether the design of the **AP1000®** design reduces the risk of violation behaviour As Low As Reasonably Practicable (ALARP).

9. My assessment approach has included three main areas of focus, which are described in detail in Subsection 4.1. In brief, these include:

- HFI: with a view to confirming the completeness of the HF Safety Case and HBSCs included for assessment as part of this issue,
- Human Error Analysis (HEA): with a view to ensuring the adequacy of the qualitative substantiation of important operator actions and the appropriate treatment of error mechanisms, misdiagnosis, and violation potential
- sensitivity of the design and safety analyses to the HBSCs: with a view to better understanding the risk importance of the HBSCs and ensuring a proportionate approach to their assessment.

10. Within my assessment I did not deem it necessary to assess every HBSC. Instead, I have elected to use a risk informed sampling approach; this is consistent with ONR practice. This sampling approach is described in Subsection 1.3.1.

11. While a sampling approach can provide a proportionate level of regulatory scrutiny, there is always a risk that issues are left unrevealed in the areas not sampled. To mitigate this risk, and to support my judgement, I have included assessment of HFI. As part of this I have considered the credibility of the Westinghouse HF capability along with the methods and processes employed. I did this to provide confidence that the risk from human error has been adequately understood, modelled and reduced So Far As Is Reasonably Practicable (SFAIRP) for the GDA of the **AP1000®** design.

1.3 Method

12. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref 3).

1.3.1 Sampling strategy

13. It is rarely possible or necessary to assess a safety submission in its entirety and therefore ONR adopts an assessment strategy based on sampling. The sampling strategy for assessment of this issue was informed by both quantitative and qualitative considerations and builds on the criteria which ONR agreed with Westinghouse in Step 4 and which were used to select human actions for assessment.

14. The quantitative criteria agreed are risk-based and include consideration of Risk Achievement Worth (RAW) and Risk Reduction Worth (RRW) with defined levels in relation to each of these measures which prompt inclusion of human actions within the sample for assessment (See Annex 1). These are further supplemented by a number of qualitative factors for example where actions are complex, unique or potentially challenging or when actions are required to prevent conflicting safety goals. Details of the criteria and definitions of RAW and RRW are presented in Annex 1.

15. The application of the screening criteria at Step 4 produced a set of 20 HBSCs which may be considered to be representative of each of the three International Atomic Energy Agency (IAEA) human error classes as outlined below:

- Type A: Human actions before the initiating event during normal operation that degrade system availability;
- Type B: Human actions that contribute to initiating events; and
- Type C: Human actions that occur post–fault.

16. With agreement from ONR, Westinghouse proposed the analysis of these 20 HBSCs covering a range of Type A, B and C errors and these formed the basis of Westinghouse's analysis and in turn the focus of errors for consideration in relation to this issue. The purpose of this sample set was to: a) provide confidence in the analysis method, and b) to identify whether further analysis was needed to close GDA)

17. Within my sampling, I have included consideration of all 20 of these initial HBSCs, plus further detail on additional / modified HBSCs which meet these criteria (See Annex 1) derived as part of Westinghouse's subsequent work in relation to this issue. In considering this sample of HBSCs I have drawn extensively on the HEA initially provided by Westinghouse and have supported this with evidence from other key sources. This has included:

- the Integrated Systems Validation (ISV) trials of the Main Control Room (MCR) and Remote Shutdown Room (RSR);
- the at-power Probabilistic Safety Analysis (PSA);
- a site inspection of the **AP1000®** reactor MCR simulator; and
- additional Westinghouse HEA developed in support of interactions with ONR during my assessment.

18. Further details of the quantitative and qualitative screening criteria are presented in Annex 1 along with a listing of the 20 HBSCs included for assessment.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

19. ONR's GDA Guidance to Requesting Parties (http://www.onr.org.uk/new-reactors/ngn03.pdf) (Ref. 4) states that the information required for GDA may be in the form of a PCSR. Technical Assessment Guide (TAG) 051 sets out regulatory expectations for a PCSR (http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf) (Ref. 5).

20. At the end of Step 4, ONR and the EA raised GDA Issue CC-02 (http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the **AP1000®** design reference point.

21. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue CC-02 and therefore this report does not discuss the HF aspects of the PCSR. This assessment focuses on the supporting documents and evidence specific to GDA Issue GI-AP1000-HF-01.

2.2 Standards and Criteria

22. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) (Ref. 6), internal TAGs (Ref.7), relevant national and international standards, and other sources of Relevant Good Practice (RGP) informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

2.2.2 The key SAPs applied within the assessment are included within Table 1. The complete list of SAPs relevant to my assessment is included in Annex 2.

Table 1: Key Safety Assessment Principles used during the assessment

SAP No	SAP Title	Description
EHF.1	Integration within design, assessment and management	A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility's lifecycle.
EHF.2	Allocation of safety actions	When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.
EHF.3	Identification of actions impacting safety	A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.
EHF.4	Identification of administrative controls	Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.
EHF.5	Task analysis	Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute.
EHF.6	Workspace design	Workspaces in which operations (including maintenance activities) are conducted should be designed to support

SAP No	SAP Title	Description
		reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors.
EHF.7	User interfaces	Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.
EHF.8	Personnel competence	A systematic approach to the identification and delivery of personnel competence should be applied.
EHF.9	Procedures	Procedures should be produced to support reliable human performance during activities that could impact on safety.
EHF.10	Human reliability	Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.
EHF.11	Staffing levels	There should be sufficient competent personnel available to operate the facility in all operational states.
SC.4	The regulatory assessment of safety cases, safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
EKP.5	Safety measures	Safety measures should be identified to deliver the required safety function(s).
ERL.3	Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.

2.2.3 Technical Assessment Guides

23. The TAGs that have been used as part of this assessment are set out in Table 2. (See Ref. 7)

Table 2: TAGs used as part of this Assessment

TAG No	Description
T/AST/005	ND Guidance on the demonstration of ALARP
T/AST/009	Maintenance, inspection and testing of safety systems, safety-related structures and components.
T/AST/010	Early initiation of safety systems
T/AST/027	Training and assuring personnel competence
T/AST/030	Probabilistic Safety Analysis (PSA)
T/AST/051	Guidance on the purpose, scope and content of Nuclear Safety Cases
T/AST/058	Human Factors Integration
T/AST/059	Human Machine Interface
T/AST/060	Procedure design and administrative controls
T/AST/060	Staffing levels and task organisation
T/AST/063	Human Reliability Analysis
T/AST/064	Allocation of Function between human and engineered systems

2.3 Use of Technical Support Contractors

24. Technical Support Contractors were not used to support my assessment.

2.4 Integration with Other Assessment Topics

25. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues which cut across multiple topics or issues. The following cross-cutting issues have been considered within, and have informed, my assessment:

- GI-AP1000-CC-03 Consider and action plans to address the lessons learnt from the Fukushima event (Ref. 8).
- GI-AP1000-ME-01 Squib valve concept and design substantiation (Ref. 9).
- GI-AP1000-PSA-02 Fire PSA (Ref. 10).

26. In order to reduce the analysis burden on Westinghouse, it was agreed that some of the HBSCs analysed to close GI-AP1000-HF-01 could be selected on the basis that they would support the closure of other GDA issues.

27. I have also had interactions with other technical disciplines as part of the closure of other GDA issues. My input into these areas is captured within the issue specific GDA reports.

2.5 Out-of-scope Items

Table 3 sets out the items which have been agreed with Westinghouse as being outside the scope of GDA and which will be addressed within licensing. Issues relating to the PCSR are also outside the scope of this assessment and are reported separately.

Table 3: Out-of-scope Items addressed during licensing

#	Item
	Site specific considerations, for example:
1.	Training – Westinghouse has provided assumptions in this area
2.	Procedures – Westinghouse has provided assumptions in this area
3.	Personnel levels – Westinghouse has provided assumptions in this area
4.	Off-site responses – Westinghouse has provided assumptions in this area
5.	Emergency Control Centre and associated role and interactions with the plant

3 REQUESTING PARTY'S SUBMISSIONS IN RESPECT OF ISSUE GI-AP1000-HF-01

28. This section provides details of the submission provided by Westinghouse to address GDA Issue GI-AP1000-HF-01.A1 - Completeness of the HF Safety Case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential.

29. This includes:

- an overview of Westinghouse's closure strategy;
- details of Westinghouse's submission over the course of the assessment period; and
- a summary of key HF related aspects of the safety case.

3.1 Summary of Closure Strategy

30. Westinghouse's closure strategy for GI-AP1000-HF-01.A1 is documented within Ref. 2. It proposed that Westinghouse would take the following actions to support the closure of GDA issue GI-AP1000-HF-01:

- Westinghouse's facilitation of the ONR review through delivery of a Human Factors Safety Case roadmap, appropriate and timely responses to Regulatory Queries (RQs), attendance at meetings, and provision of requested supporting documentation.
- Perform a systematic assessment of HFI across the remaining 50 GDA Issues.
- Perform a human factors review of selected **AP1000®** Design Change Proposals to identify any human actions created as part of the design changes approved by Westinghouse since the Reference Date of 16 September 2010.
- Assure human error identification completeness and assess the potential use of optimistic claims through:
  - Review, and revision as required, of existing **AP1000®** design Human Factors Safety Case supplemental documents to UKP-GW-GL-042, Revision 0 (Ref. 11).
  - Use of a sampling plan approach for the review of claims on operator actions; substantiating the claims where possible and identifying assumptions. Where substantiation of claims is not possible, qualitatively reassess the action consequences.
  - Incorporate assessment, results, and findings from these efforts into subsequent revisions to the **AP1000®** design PCSR, UKP-GW-GL-793 (Ref. 12)

3.2 Details of Westinghouse's Submission

31. It is important to note that work to address GDA Issue GI-AP1000-HF-01 has taken place over a period of ~ 2 years and has comprised a number of discrete HEA submissions by Westinghouse. In addition to the initial documentation, in subsequent interactions with Westinghouse has also provided revised analysis and important additional evidence from other sources, including HF ISV trials, and wider supplementary information.

32. The following section provides an overview of the documents and evidence submitted with more extensive supporting information provided in Annex 3. This includes listings of the individual HBSCs considered.

33. Westinghouse applied a number of HEA methods during the course of the **AP1000®** design GDA. To aid understanding I have classified these methods and submissions into three phases.

3.2.1 Phase 1

34. Phase 1 was submitted in early 2011. The submission was made to address the ROs which were later combined into GI-AP1000-HF-01. It fell outside ONR's Step 4 assessment window so was not formally assessed. It comprised the following documentation:

- UKP-GW-GL-069, Rev. 0, "Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 PRA Update". 7 HBSCs analysed (Ref. 13).
- UKP-GW-GL-070, Rev. 0, UK AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA. 6 HBSCs analysed (Ref. 14).
- UKP-GW-GL-071, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 Low Power and Shutdown PRA. 9 HBSCs analysed (Ref. 15).
- UKP-GW-GL-072, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Potential Improvements As Proposed in the ALARP Analysis. No HBSCs analysed (Ref. 16).
- UKP-GW-GL-073, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Identified Non-Core Damage Human Errors with Possible Radioactive Release. 6 HBSCs analysed (Ref. 17).
- UKP-GW-GL-074, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability. No HBSCs analysed (Ref. 18).
- UKP-GW-GL-075, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults. 9 HBSCs analysed (Ref. 19).
- UKP-GW-GL-076, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms (Ref. 20). 12 HBSCs analysed

3.2.2 Phase 2

35. The Phase 2 HEA submission was produced to address ONR feedback (Refs. 21-22) on the Phase 1 HEA. It used the latest iterations of the **AP1000®** PSA and the sampling approach described in Subsection 1.3.1 to identify 20 HBSCs for detailed analysis; some new, some previously assessed in Phase 1. This was submitted in mid-2016 and was split across two documents supporting the closure of both GI-AP1000-HF-01 and GI-AP1000-CC-03. These two documents form the principle paper-based HEA submission:

- UKP-GW-GL-126 – Revision 0 - United Kingdom AP1000 Human Factors Qualitative Error Analysis (Ref. 23); and
- UKP-GW-GGR-201 – Revisions 1 – UKAP1000 Plant Post-Fukushima (Ref. 24).

36. UKP-GW-GL-126 (Ref. 23) contains the following:

- an explanation of how the HBSCs were selected for detailed HEA;
- a description of the assumptions made that underpin the HEA, i.e. Conduct of Operations, procedural use and adherence, staffing, training, human performance, safety culture, HSIs, and miscellaneous;

- An assessment of diagnostic error;
- An assessment of violation potential; and
- An assessment of the following Type A, B, and C errors:
  - Type A: HEPE-PCS-XVM-CL-V023 – Passive Containment Coolant System (PCS) manual valve PCS-PL-V203 unintentionally left closed;
  - Type C: HEP-ADS4-C1 Operator fails to depressurise the Reactor Coolant System (RCS) with Automatic Depressurisation System (ADS) Stage 4 on low Core Make-up Tank (CMT) level;
  - Type C: HEPO-COG-CONT Operator fails to diagnose high containment pressure;
  - Type C: HEPO-COGCORECOOLING - Operator fails to diagnose inadequate core cooling;
  - Type C: HEPO-FI-ADSDIS Operator fails to open breakers to prevent spurious ADS Stage 4 actuation;
  - Type C: HEPO-FI-MCREVAC Main control room evacuation due to fire;
  - Type C: HEPO-INJ Operator fails to actuate In-containment Refuelling Water Storage Tank (IRWST) injection;
  - Type C: HEPO-L2-CAVFLD Operator fails to flood Reactor Vessel (RV) cavity for IVR on loss of core cooling cue;
  - Type C: HEPO-L2-CNT Operator fails to manually isolate containment;
  - Type C: HEPO-L2-H2I Operator fails to manually actuate hydrogen ignitors;
  - Type C: HEPO-OFILL Operator fails to isolate ruptured Steam Generator (SG) (on High-3 NR SG level – Protection and Safety Monitoring System (PMS) backup);
  - Type C: HEPO-PRHR-GT Operator fails to actuate Passive Residual Heat Removal (PRHR) during an event without a Safeguards signal;
  - Type C: HEPO-RNSINJ Operator fails to align Normal Residual Heat Removal System (RNS) for injection;
  - Type C: HEPO-RRWSTISO Operator fails to isolate IRWST recirculation following spurious recirculation actuation;
  - Type A: OPR-011 Maintenance error leads to failure of ADS Stage 4 and IRWST gravity injection squib valves;
  - Type B: OPR-099 Operator incorrectly executes the CMT discharge valves operability test.
  - Type A: OPR-106 Maintenance error leads to failure of recirculation squib valves; and
  - Type B: OPR-131 Operator improperly seats the fuel assembly within the core.

37. UKP-GW-GGR-201 (Ref. 24) presented two beyond design basis (BDB) HBSCs selected using the same screening criteria:

- BDB-005 Operators provide makeup to the Passive Containment Cooling Water Storage Tank (PCCWST) and Spent Fuel Pool (SFP) from the Passive Containment Cooling Auxiliary Water Storage Tank (PCCAWST) with the offsite pump; and
- BDB-006 Operators provide makeup to the SFP by gravity drain from the PCCWST.

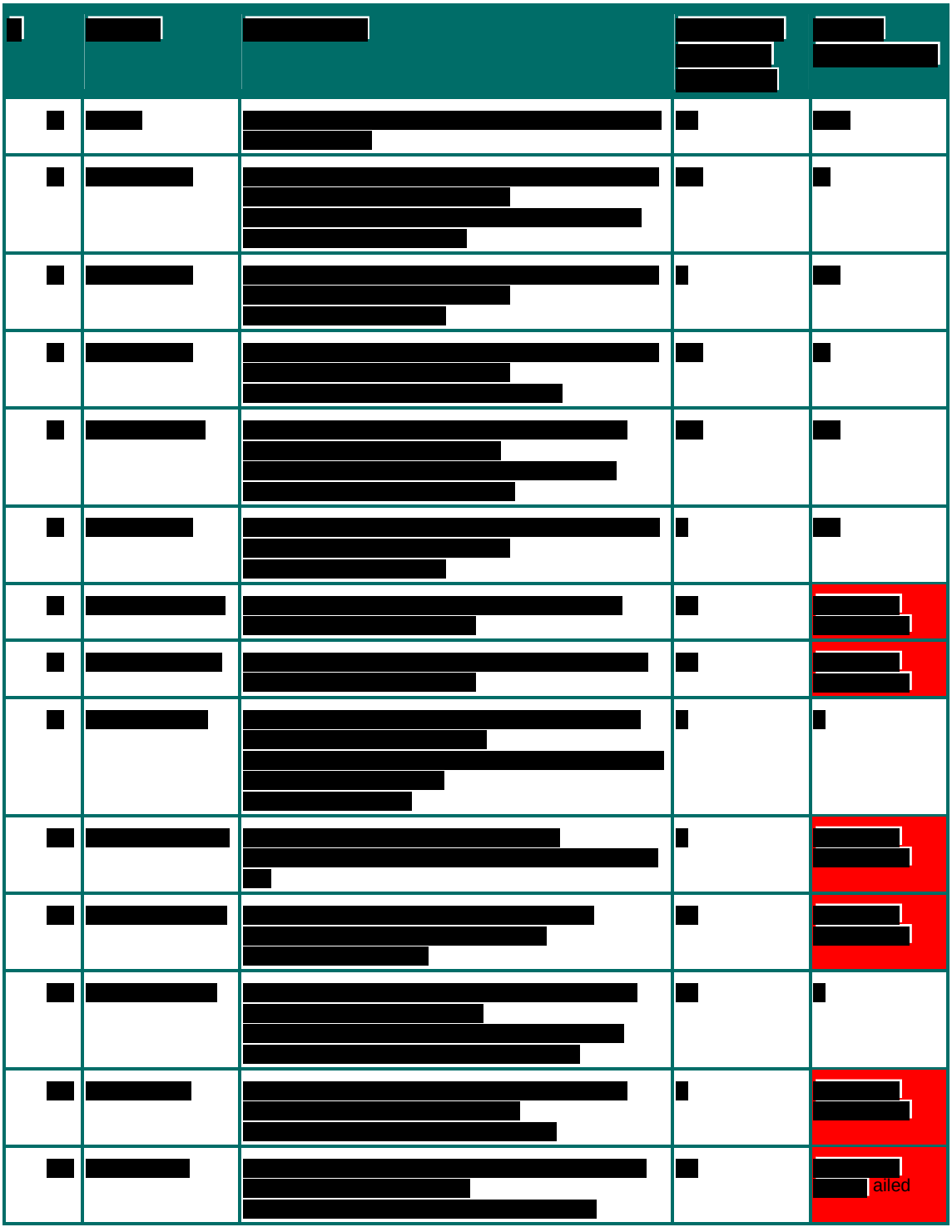
38. On the advice of ONR, and prior to the delivery of the Phase 2 analysis, in January 2016 Westinghouse also submitted the results of ISV trials as supplementary evidence. The ISV trials analysed the efficacy of MCR / RSR HSI ensemble. They were conducted on a full-scope simulation facility using Suitably Qualified and Experienced Personnel (SQEP) **AP1000®** PWR operators supplied by domestic US utilities. The results are presented in:

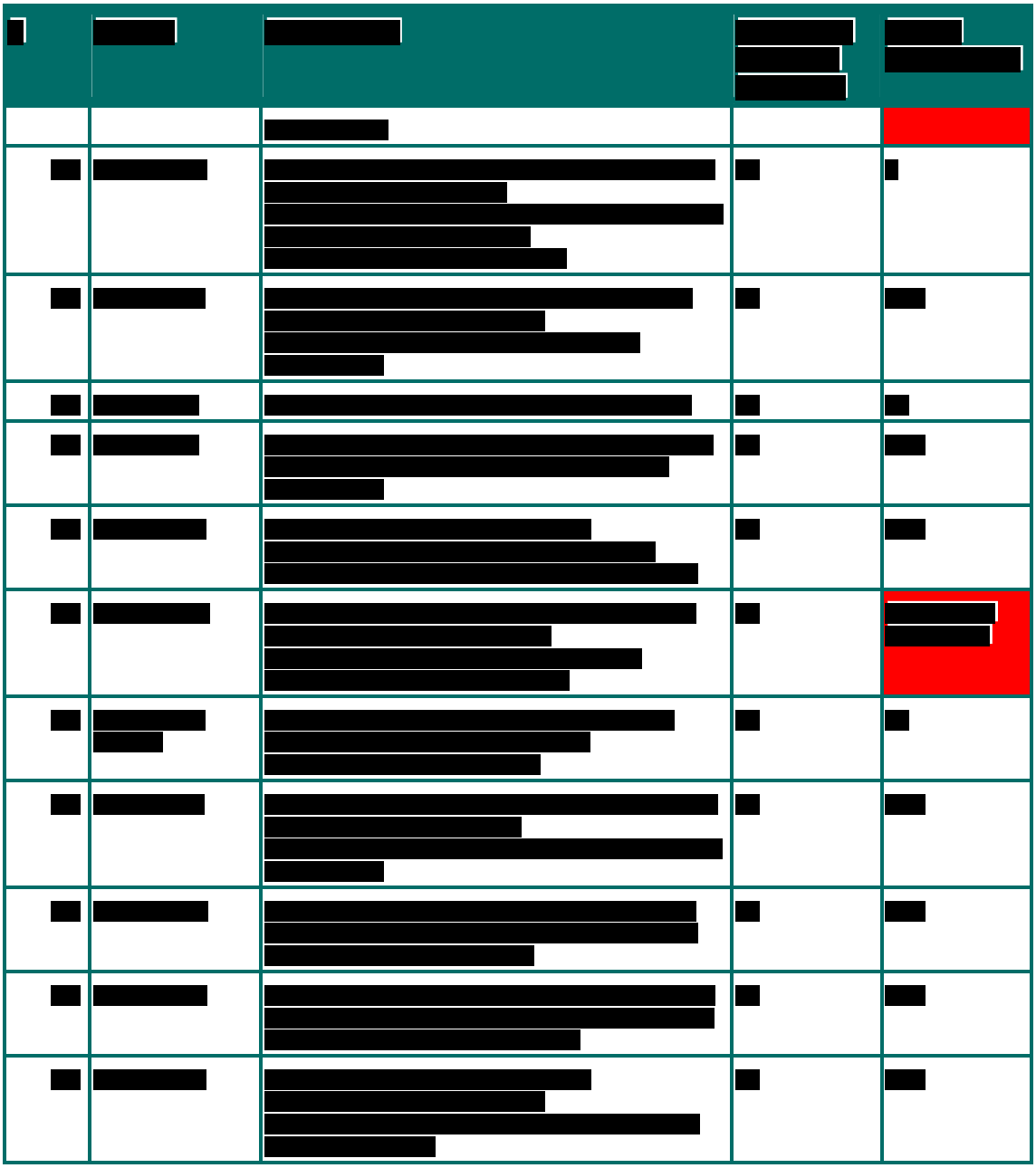
  - APP-OCS-GER-320 Rev 0, September, 2015 AP1000 Human Factors Engineering Integrated System Validation Report (Ref. 25).

39. This report describes the scope of the trials, the scenarios used for evaluation purposes, and the conclusions; either validation of the HSI features or identification of Human Engineering Deficiencies (HEDs) for further resolution. In all, 23 scenarios were used, and these were run a minimum of three times or a maximum of four; a fourth trial was scheduled if one of the preceding trials failed. The scope of the evaluation scenarios are presented in Annex 4.

40. During the 23 scenarios, the following HBSCs (Risk Important Human Actions – RIHA) were tested. Failures by crews to achieve the required actions does not in itself, undermine confidence in the HSI design; ISV trials provide the opportunity to validate the HSI and to identify potential for design iteration.

Table 4: Risk Important Human Actions Tested During the ISV Trials





41. The ISV trials report (Ref. 25) concluded that:

42. "*Through the performance of 3 to 4 trials of the 23 scenarios, 62 Human Engineering Deficiencies (HEDs) were identified where requirements were not met; however, it is concluded that the given plant operations were performed and necessary tasks were completed such that the health and safety of the public would not be challenged and that the integrated system supports the safe operation of the plant.*"

43. Westinghouse claimed that the test and analysis results demonstrate that the MCR operators could perform the following:

- heat up and start up the plant to 100% power;
- shut down and cool down the plant to cold shutdown;
- bring the plant to safe shutdown following the specified transients:
  - reactor trip; and
  - turbine trip.
- bring the plant to a safe, stable state following the specified accidents:
  - small-break LOCA;

- large-break LOCA;
- steam line break – steam line and feed water breaks;
- feed water line break; and
- steam generator tube rupture.

3.2.3 Phase 3

44. Due to feedback from ONR that References 23 and 24 would not be sufficient to fully close out GDA issue GI-AP1000-HF-01, Westinghouse provided supplementary analysis in November / December 2016 in three areas; It enhanced the analysis of misdiagnosis and violation potential and re-analysed three of the HBSCs within in UKP-GW-GL-126. This new analysis was performed using an improved HEA method. These submissions comprised:

- Westinghouse-REG-1432N – Enclosure 1 – Misdiagnosis Potential (Ref. 26)
- Westinghouse-REG-1432N – Enclosure 2 – Violation Potential (Ref. 27)
- Westinghouse-REG-1477N – Enclosure 1 – Revised Human Error Analysis (Ref. 28)
  - OPR-099: Operator executes the core make-up tank discharge valve operability test.
  - HEPO-FI-ADSDIS: Operator prevents fire-damage-related hot-shorts from spuriously generating the signals necessary to actuate and open the automatic depressurisation system fourth stage squib valves.
  - OPR-011: Operators conduct testing and maintenance on the 14-inch automatic depressurisation system fourth stage squib valves.

3.3 Summary of the Safety Case

45. The **AP1000®** reactor design is an evolved and up-scaled version of the Westinghouse **AP600**® Pressurised Water Reactor (PWR) nuclear power plant design. The design differs from current GB nuclear power stations in that it is a passive plant concept. A passive plant is one where the need for Alternating Current (AC) to power safety systems is removed. Instead, energised systems are powered by alternative means such as Direct Current (DC) stored in batteries, compressed air, pyrotechnic-actuation, and gravity feeds, etc. It also features passive heat removal strategies that employ natural circulation / convection / evaporative / gravity-fed cooling systems that initiate following the failure of active duty cooling systems.

46. An additional feature claimed for the **AP1000®** design is that it de-emphasises the role of the operator during anticipated operational occurrences, design basis accidents, beyond design basis accidents, and severe accidents. One of the key **AP1000®** design criteria is “no operator actions for safety functions” (Ref. 29) and Westinghouse states that the evidence from the probabilistic risk model supports this (Ref 30).

47. In the period between the end of GDA Step 4 and this assessment period, Westinghouse has revised its claims, arguments and evidence structure in line with better understanding of regulatory expectations and the evolution of the design. The overarching HF safety claim for the **AP1000®** design is now:

- Claim 0 - The role of the operator in ensuring nuclear safety is understood, and the risk to nuclear safety arising from human failure has been identified and reduced ALARP for the UK Standard **AP1000®** plant design. (Ref. 12).

48. The overarching claim is underpinned by a hierarchy of sub-claims of which only the top tier are reproduced here:

- Claim 1 - The implementation of a comprehensive, integrated and managed Human Factors Engineering Programme promotes high levels of confidence in the ability of the Standard **AP1000®** plant design to support successful completion of the operational tasks and maintenance activities important to safety and assigned to the human operator.

- Claim 2 - The design of the MCR and of the HSI supports safe and reliable operations during normal modes of operation, and in abnormal and emergency conditions and recovery operation during severe accident (ie core-damage).

- Claim 3 - The design and operating philosophy for the Standard **AP1000®** plant design reduces reliance on operator action to ensure nuclear safety and reduces the sensitivity of the plant to human error.

- Claim 4 - The plant procedures, including the Conduct of Operations, applied to the Standard **AP1000®** plant design support safe and reliable operation during normal operation, abnormal operation, and emergency conditions.

- Claim 5 - The HBSCs, identified as part of the Design Basis Analysis (DBA), PSA and Severe Accident Analysis (SAA), have been substantiated ALARP.

- Claim 6 - A sample of Type A, B and C errors have undergone cognitive-level HEA to identify credible error modes and mechanisms (root cause) and performance shaping factors so that error reduction mechanisms can target the risk of failure ALARP for the Standard **AP1000®** plant design.

- Claim 7 - The symptom-based approach of the Emergency Operating Procedures (EOPs) and of the incontrovertibly different entry conditions to each EOP has reduced the potential for diagnostic error such that it is considered to be reduced ALARP for the Standard **AP1000®** plant design.

- Claim 8 - The equipment design, task or operating context conditions that may cause behaviour in violation of procedures have been identified through HEA analysis or observed during the HF ISV test. Respective ISV HEDs have been identified. Resolution of these HEDs shall be agreed upon, implemented, and re-verified/re-validated such that the risk for violation is ALARP.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-HF-01

49. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 32).

4.1 Scope of Assessment Undertaken

50. The purpose of the GDA process is to determine whether a reactor design is capable of being built and operated in Great Britain, on a site bounded by a generic site envelope, in a way that is acceptably safe and secure.

51. A DAC is issued when the ONR and the EA are confident that sufficient information has been provided, and that no significant safety, environment or security issues have been identified that cannot be resolved. Thus, it would be disproportionate to expect a fully resolved design and safety case at this stage in the **AP1000®** design GB build programme.

52. The scope of GI-AP1000-HF-01 relates to the completeness of the HF safety case, specifically in the areas of human error mechanisms, operator misdiagnosis potential and violation potential. This includes:

- Type A Human Errors (Pre-Initiators, e.g. maintenance errors);
- Type B Human Errors (Initiators, e.g. human-Initiated events);
- Type C Human Errors (Post-Initiators, e.g. human errors whilst performing safety actions or actions that aggravate a fault sequence);
- Misdiagnosis Errors; and
- Violation Potential.

53. My assessment has included review of the outputs from Westinghouse’s GDA Issue Resolution Plan supported by consideration of additional evidence from Westinghouse’s wider design and safety case analyses. In undertaking my assessment I have focussed on three main areas of consideration. These are:

- HFI; with a view to confirming the completeness of the HF Safety Case and HBSCs included for assessment as part of this issue;
- HEA; with a view to ensuring the adequacy of the qualitative substantiation of important operator actions and the appropriate treatment of error mechanisms, misdiagnosis and violation potential; and
- Sensitivity of the design and safety analyses to the HBSCs; with a view to better understanding the risk importance of the HBSCs and ensuring a proportionate approach to their assessment.

54. In addition, the Step 4 HF report (Ref. 33) raised a number of assessment findings which require additional Human Factors Analysis (HFA) relating to identification and substantiation of HBSCs. These will be undertaken during licensing and I have given cognisance to them in undertaking my assessment. Details of the findings can be found in Annex 5. In addition, where minor outstanding concerns are identified in my assessment, I have also, where appropriate, cross-referenced these to the relevant HF assessment findings from Step 4 to ensure an integrated approach with regard to HF in the future.

55. I have also taken into account the credibility of the Westinghouse HF capability and HFI process as these two organisational enablers are key to delivering effective HEA for GDA and in the future support of **AP1000®** design site licensing. This is an important consideration when using a sampling based approach.

56. I have also, across the period of the assessment, had a number of interactions with Westinghouse to discuss and clarify aspects of the issue and have followed these up with RQs. These are referenced where appropriate in the upcoming sections.

57. For further information on ONR's regulatory assessment of the totality of the HF contribution to the design of, and Safety Case for, the **AP1000®** design, see ONR's Step 4 assessment report (Ref. 33).

4.2 Assessment of Human Factors Integration

58. It was important to take into consideration HFI with a view to confirming the completeness of the HF Safety Case and HBSCs included for assessment as part of this issue.

59. The following sections outline my opinions and judgement on Westinghouse's HF capability and HFI processes. These have been used to inform my view on Westinghouse's ability to deliver a cogent and coherent HF Safety Case and its completeness in relation to consideration of the HBSCs.

4.2.1 Organisational HF Capability

60. At the start of my interactions with Westinghouse it was clear that it possessed a highly credible HF design capability, as demonstrated by the HFI applied to the design of the MCR / RSR. These early interactions, however, identified capability limitations relating to the ability to deliver GB-relevant modern standards HEA. Westinghouse recognised this limitation and recruited a specialist in this area.

61. I have interacted with the Westinghouse HF team regularly over the last two years, including an inspection of the **AP1000®** PWR simulator over the course of a week. In that time, the behaviours I observed, and the knowledge and competence demonstrated in the field of human factors, was exemplary. I consider that the limitations I raised during the course of my interactions were largely due to the different regulatory frameworks that exist between GB and the United States (US) and that, once a shared understanding had been established, they were quickly addressed, or a way forward was arrived at. The composition of the team is balanced, drawing together experts from both operational and academic backgrounds. Westinghouse also sought to enhance its GB-specific knowledge in the area of HF through the use of UK-based HF consultants.

62. During interactions between Westinghouse and ONR (PSA and HF inspector) in July 2015, it became clear that there were limitations in the integration between the Westinghouse PSA and HF disciplines – as described in Reference 34. In particular, there was a disconnect between the qualitative HEA work and the quantitative Human Reliability Analysis (HRA) used in the PSA. Following an intervention by ONR, Westinghouse committed to address this limitation fully during licensing and partially during GDA. All qualitative HF analyses will be performed by the HF team and resultant data will then be used as the basis for the derivation of Human Error Probabilities (HEPs) by the PSA team (Ref. 35). Westinghouse has committed to formalise these interactions in a Level 3 **AP1000®** design project procedure and project quality plan. Its commitments included the following:

- To update all human actions in the Human Action Database (HAD), including collecting the minimum set of information for screened-out actions, which will facilitate adequate bounding case ALARP justifications for screened out-actions.
- To work with PSA to sentence the human actions found in the HF human action database (resulting from the HF GDA activities) with respect to inclusion in the site licensing PSA update.

- To conduct a complete, modern-standards qualitative analysis of the human actions that pass through the screening criteria, with appropriate documentation via the pro-forma template established and approved during GDA.
- To provide the qualitative analyses to the PSA staff, who will calculate final HEPs based on the HF qualitative analyses to update the PSA accordingly.
- To conduct individual ALARP assessments for the human actions that pass through the screening criteria. Ensuring that screened-out actions receive appropriate ALARP assessment, via bounding case arguments.
- To work with the PSA staff to address the numerous HRA-related findings from the PSA GDA Step 4 report and the HF GDA Step 4 report. There are 4 HRA-related findings assigned to the PSA, and 22 HRA-related findings assigned to the HF discipline. The HF and PSA teams will work together to ensure that these findings are appropriately addressed.

63. Based on the above, I consider Westinghouse has a highly competent HF design and safety capability with which to support the licensing of the **AP1000®** design.

4.2.2 HFI process

64. A full review of Westinghouse's HFI process was previously conducted during Step 4 (Ref. 33). It concluded that there was little evidence of a fully integrated programme that actively worked with other related technical disciplines in a cohesive manner to optimise the design, and develop and iterate the safety analysis. Where HFI was strong was input to the design of the MCR and RSR. I recognised these same limitations when I started my interactions with Westinghouse in 2014/2015.

65. In October 2014, when Westinghouse re-engaged with the GDA process, presentation was made to ONR on each of the 51 GDA issues, explaining the closure strategy for each. In the HF discipline, Westinghouse's position at that time was that:

- no additional analysis was likely as it had supplied UKP-GW-GL-076 (Ref. 20) at the end of Step 4, which had yet to be assessed by ONR; and
- no additional HF support would be required to close out the other GDA issues.

66. During the presentation, I advised Westinghouse that based upon a high-level review of this submission, this was not a credible position to take and I followed this up with RQ-1293 (Ref. 21), asking how Westinghouse would ensure that HFI was managed appropriately across all 51 GDA issues. I also queried (Ref. 22) how the body of work submitted by Westinghouse at the end of Step 4 fitted together to present a cogent and coherent safety case, in line with the expectation of TAG-051 (Ref. 7).

67. Between November 2014 and January 2015 I undertook a high level assessment of the totality of work submitted along with some supporting documents that had informed the Step 4 assessment. The result of this assessment was RQ-1308 (Ref. 36) which provided feedback to Westinghouse on the limitations of the current method of HEA. Westinghouse responded by committing to address the specific limitations as part of its resolution plan.

68. Westinghouse responded to this early intervention by committing to:

- an HF review of all 51 GDA issues to identify any new HBSCs and HF support work. This was delivered against by Reference 37 and Reference 38;
- a review of all DCPs to identify any new HBSCs and necessary HF support work, which Westinghouse delivered against (Ref. 39);
- the provision of a road-map for the HF Safety Case; over time this evolved into the claims, arguments, and evidence summary within the HF chapter in the **AP1000®** design PCSR; and

- the provision of additional HEA addressing the limitations identified by ONR; this analysis was later submitted in UKP-GW-GL-126 (Ref. 26).

69. The two reviews described above identified 92 (Ref. 38) and 25 (Ref. 39) HBSCs to add to the HAD for further screening and analysis. Both of these activities demonstrate an effective HBSC identification process.

70. Westinghouse responded well to ONR's interventions relating to HFI and, as a result, Westinghouse made some significant improvements with respect to meeting GB regulatory expectation for effective HFI. Improvements included:

- a significant increase in HF support to the closure of other GDA issues, as evidenced by HF attendance at cross-cutting meetings;
- non-HF disciplines actively seeking HF support;
- Westinghouse committed to addressing the limitations of the working practices between the HF and PSA disciplines (Ref. 35; see also section 4.2.1); and
- Westinghouse identified an extant limitation in its HFI process: there wasno requirement for HFI into Commercial-Off-The-Shelf (COTS) equipment.

71. The focus of HF effort to date has been on the primary interfaces contained within the MCR and RSR and this has had a positive impact on the HSI design. Over the last two years, a number of limitations have been identified in the HF associated with local task-designs and interfaces. For example, the task-design for the maintenance of squib-valves and the lack of HFI into COTS equipment indicated that further HFI into the design of local systems, structure and components was required. This will be addressed under Step 4 Assessment Finding AF-AP1000-HF-44 - The licensee shall provide formal arrangements for HFI with other technical disciplines as part of the HFIP for UK construction of the **AP1000®** design.

72. I consider that Westinghouse has an extremely strong HFI process supporting the design and analysis of the MCR and RSR. Integration of HF into other areas of the design is rapidly improving and I welcome the significant commitments made to further improve HFI during licensing in the design and safety analysis areas. I also note the willingness of non-HF disciplines to seek out HF support during the resolution of non-HF GDA issues. This provides good evidence of improved HFI and in combination with the further work which will be undertaken to address Step 4 assessment finding AF- AP-1000-HF-44, gives confidence that HFI will continue to improve during licensing so that it fully meets regulatory expectations

4.2.3 HFI Conclusions

73. In general, I found that Westinghouse made significant improvements in the integration of HF and that processes now adequately supports the identification and analysis of HBSCs. In particular, I note that Westinghouse has expanded its scope by reviewing all 51 GDA issues for additional previously unidentified HBSCs. Westinghouse has also proportionately reviewed all DCPs and this has also identified additional HSBCs. This gives confidence in the rigour and completeness of the HBSC identification.

74. I found that HBSCs are managed via Westinghouse's HAD and I am content with Westinghouse's method for selecting HBSCs from the human action database for further detailed analysis and substantiation. I have reviewed the method and underpinning criteria and judge that it combines risk and representativeness to inform the selection of HBSCs which I consider to be a sensible and proportionate approach.

75. In addressing this issue I note that Westinghouse responded constructively to challenges made by ONR and put considerable time and effort into the development of expertise in this area. As a result, it is my view that Westinghouse has developed a credible and responsive HF design and analysis capability. This is important in

supporting the effective deployment of HFI, the reliable identification of HBSCs, and ultimately in supporting the licensing of the **AP1000®** design.

4.3 Assessment of Human Error Analysis

76. ONR expects that HEA is presented in a cogent and coherent manner. Usually, this is as a single document, or via a suite of analyses that is then summarised into a head document that articulates the higher level claims and arguments and provides a road-map to the evidence.

77. This has not been the case with Westinghouse's submission and it has been necessary to draw together and integrate multiple sources of evidence which has complicated my assessment.

78. My assessment of Westinghouse's HEA considers the analysis performed during the two year period of my assessment including the three phases of submission outlined in Section 3. It also draws upon the results of the ISV trials and the latest iteration of the at-power PSA.

79. In the following sections I will discuss:

- The limitations of the HEA submitted in Phases 1 and 2;
- The adequacy of the Phase 3 HEA;
- The confidence that can be drawn from the ISV trials;
- The adequacy of the analysis of violation potential; and
- The adequacy of the analysis of misdiagnosis potential.

80. My consolidated judgements are presented at the end of this section.

4.3.1 AP1000® design Phase 1 HEA

81. Phase 1 was submitted in early 2011. The submission was made to address the ROs which were later combined into GI-AP1000-HF-01 and represented a significant body of work by Westinghouse. It fell outside of ONR's Step 4 assessment window so was not formally assessed. It is comprised of the following new and updated documentation:

- UKP-GW-GL-069, Rev. 0, "Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 PRA Update". 7 HBSCs analysed (Ref. 13).

- UKP-GW-GL-070, Rev. 0, UK AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA. 6 HBSCs analysed (Ref. 14).

- UKP-GW-GL-071, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 Low Power and Shutdown PRA 9 HBSCs analysed (Ref. 15).

- UKP-GW-GL-072, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Potential Improvements As Proposed in the ALARP Analysis. No HBSCs analysed (Ref. 16).

- UKP-GW-GL-073, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Identified Non-Core Damage Human Errors with Possible Radioactive Release. 6 HBSCs analysed (Ref. 17).

- UKP-GW-GL-074, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability. No HBSCs analysed (Ref. 18).

- UKP-GW-GL-075, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults. 9 HBSCs analysed (Ref. 19).

- UKP-GW-GL-076, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms (Ref 20). 12 HBSCs analysed

82. I assessed these at the start of 2015 and found a number of limitations in the analysis. While it was clear that it had been performed by SQEP HF and operations personnel, each of the submissions was lacking in sufficient cogent detail to provide evidence to close GI-AP1000-HF-01. I advised (Ref. 36) Westinghouse of the following:

- The level of task detail was insufficient to inform the identification of credible human errors, e.g. who is doing the task, where this task is being by performed, using what equipment / interfaces, and how long the task takes - if time pressure is likely to be a relevant Performance Shaping Factor (PSF).
- It was difficult to determine whether dependency between actions, personnel, and equipment had been considered.
- The analysis offered little insight into the credible errors that could occur; typically, all theoretically possible errors were listed.
- The analysis failed to describe the positive and negative PSFs and how they influenced the task.
- The analysis failed to identify socio-technical assumptions about future licensee organisation.
- The analysis failed to identify uncertainties for future validation.
- The analysis failed to explain the inter-relationships between the errors, PSFs, recovery opportunities, defences, etc.
- Where recommendations are made and rejected on ALARP grounds, the reasoning behind the rejection should be explained, either directly within the report, or via reference.
- The analysis method used was not always the most appropriate for the activity being analysed.

83. Despite the limitations described above, I did however draw some confidence from the fact that, in total, 49 HBSCs were analysed and the analysis generated sensible ALARP recommendations. This indicates that greater insight was gained from the analysis than was reported in its outputs.

84. Westinghouse responded positively to my feedback with the commitment to modify the HEA methodology to address the above limitations. This led to the submission of the Phase 2 HEA described below.

4.3.2 AP1000® design Phase 2 HEA

85. This section describes my assessment of the Phase 2 HEA presented in:

- UKP-GW-GL-126 United Kingdom AP1000 Human Factors Qualitative Error Analysis; and
- UKP-GW-GGR-201 – REVISION 1 – UKAP1000 Plant Post-Fukushima

UKP-GW-GL-126 United Kingdom AP1000 Human Factors Qualitative Error Analysis

86. Westinghouse submitted the major HEA submission in June 2016. This document represented a significant body of work, extending to over 400 pages of analysis, covering 18 HBSCs and the misdiagnosis and violation safety cases. The

misdiagnosis and violation safety case are discussed below in sections 4.3.5 and 4.3.6.

87. In order to analyse the HBSCs listed in UKP-GW-GL-126, Westinghouse developed a new methodology addressing previous weaknesses identified by ONR in Westinghouse's Step 4 submissions. This methodology was based on the NRC publication NUREG-2114, Cognitive Basis for Human Reliability Analysis (Ref. 40), and was developed by the NUREG's author. I consider this to be a sound technical basis for the development of the method.

88. The method comprised five phases (Ref. 23):

- **Stage 1 - Information gathering**, including a review of:
- Basic metadata already collected in the HAD pro-forma;
- Description of the scenario and all initial conditions;
- Any prior HF or PRA analysis of the action;
- All associated event tree(s), fault tree(s), and identification of actions from the same event sequence;
- All previous PRA of the action, including any operator interview notes;
- Success criteria;
- Any previous task analysis;
- Any previous HF assessment from the GDA Steps 3 or 4 submissions;
- All relevant procedures and supplementary documentation (these should be identified in the HAD metadata), including:
  - Type A actions: maintenance, testing, inspection, or surveillance procedures;
  - Type B actions: normal operating procedures, any relevant MTIS procedures;
  - Type C actions: abnormal, alarm response, and emergency procedures, etc.;
  - Any associated background documents, Conduct of Operations, Maintenance philosophy or standards, etc.;
  - System information, P&ID, diagrams, animated models, etc.;
  - Relevant ISV test results; and
  - Any Operational Experience/Lessons Learned.
- In this phase, the HF analysts began populating the assessment pro-forma with the scenario description information.
- **Stage 2: Task Analysis**
- Assessment team: HF analyst, operations specialist, and any other necessary team members (such as PSA):
  - Identify critical subtasks - those steps that must be completed correctly to successfully complete the action or avoid negative consequences to the plant.
  - Timing data.
  - Identification of relevant HEDs.
- **Stage 3: Error Analysis**
- Production of failure path analysis, which maps out potential plausible failures of the critical sub-tasks.
- Identification of relevant PSFs and evaluation of the state and effect of those on the operators conducting the action. In this phase, the HF analyst completed the error types/mechanisms and relevant PSFs section of the Timeline / Task Analysis table, developed a failure path diagram, and documented the PSF impact in the HEA section of the pro-forma.
- Creation of time-lines where necessary.
- In many instances, the HF team iterated several times through Phase 2 and Phase 3 before completing the Timeline/Task Analysis table and the failure path diagram.
- **Stage 4: Review and Revision**
- Review by operations specialist and any other team members (such as PSA).
- Revision based on internal review comments.
- **Stage 5: Claims-Argument-Evidence and Assessment Summary**

- Evidence (CAE) structure and a narrative assessment summary.
- Additional review and revision.
- Document assumptions for validation during site licensing.

89. The method used a pro-forma to capture the analysis of each HBSC. The fields are reproduced in Annex 6.

90. Despite the method having a sound basis, I consider that there are a number of limitations.

91. The pro-forma design segregates data that would normally be co-located. This segregation makes it difficult to relate task initiation cues, recovery opportunities, PSFs and consequences to the relevant task step. The more complex the task, the more this limitation become apparent.

92. The tabular analysis provides variable detail which does not always fully substantiate the tasks. For example, one entry in the error type field simply states “fails to understand significance”. There is no discussion as to why this might be the case, whether it is likely to occur, or what the effects of this are. In other examples, fields are simply left blank.

93. I also identified some problems in application. In one example, (the maintenance of squib valves) the analyst failed to challenge the fundamental credibility of the task. The analysis of the task was reasonable and made some sensible recommendations, but failed to identify that the basic task-design did not reduce risk ALARP. (After raising this issue with Westinghouse, the task was re-designed with input from the HF team and the analysis revisited was undertaken following the revised methodology (see subsection 4.3.3).

94. I found that the method applied in this Phase 2 HEA to be fundamentally sound with respect to its underpinnings and that the Westinghouse HF team had a high degree of competence. The analysis also made sensible recommendations to enhance risk mitigation, so the analysis was at least partially effective.

95. However, the output from this method again failed to fully deliver against regulatory expectations, as noted above. It raises the question of whether this was due to the analysis or a reporting issue. Based on my assessment of this submission, and discussions with Westinghouse, I consider that it was most likely a combination of the two. I base this on the fact that later analysis, which was developed to explicitly address the points raised above, easily met GB RGP and provides substantive evidence. Westinghouse stated that it used external contractors for some analysis which may account for the variability. This was the case for OPR-011 and may account for the lack of challenge, i.e. the contractors analysed what they were asked to, rather than challenge the basic achievability / feasibility of the task.

96. Due to uncertainties in the analysis, I was unable to recommend the closure of GI-AP1000-HF-01 based solely on the analysis presented in UKP-GW-GL-126.

97. The uncertainties in this analysis led me to:

- influence Westinghouse to develop a revised method designed to specifically address the limitations described above; and
- expand the scope of my assessment to take into account additional evidence and analyses provided by Westinghouse including the ISV trials and various PSA studies.

98. Given that the analysis presented in UKP-GW-GL-126 is largely made redundant by subsequent submissions (see list below) I will not comment further on it.

- Human Factors Engineering Integrated System Validation Report (Ref. 25)
- Westinghouse-REG-1432N – Enclosure 1 – Misdiagnosis Potential (Ref. 26)
- Westinghouse-REG-1432N – Enclosure 2 – Violation Potential (Ref. 27)
- Westinghouse-REG-1477N – Enclosure 1 – Revised Human Error Analysis (Ref. 28
- At power PSA (Ref. 30)

UKP-GW-GGR-201 – Revision 1 – UKAP1000 Plant Post-Fukushima

99. UKP-GW-GGR-201 (Ref 24) was produced to close out the cross cutting GDA issue: GI-AP1000-CC-03. This issue required the **AP1000®** design be reviewed against the lessons learned from the Fukushima accident.

100. In determining the list of HBSCs to analyse to close GI-AP1000-HF-01, I spoke with colleagues about how best to use this opportunity to align the HF work-stream to support the closure of other GDA issues. Among other examples, it was possible to select two HBSCs that would be suitable to support the closure of both GI-AP1000-HF-01 and GI-AP1000-CC-03.

101. Although reported in UKP-GW-GGR-201, the two HBSCs were analysed using the same method as that used in UKP-GW-GL-126. However, the methodological / application limitations have a lesser effect on the analysis presented in Reference 23 due to the simplicity of the tasks analysed.

102. The HBSCs analysed comprise:

- BDB-005 Operators provide makeup to the PCCWST and SFP from the PCCAWST with the offsite pump; and
- BDB-006 Operators provide makeup to the SFP by gravity drain from the PCCWST.

103. Each of the analyses is underpinned by an extremely comprehensive set of assumptions about the future licensee. For example, one of the assumptions is that dive-team support will be available should there be a need to support clearance of the site.

104. Both sets of analysis have identified sensible ALARP improvements which are being carried forward. Examples include:

- enhancing the power supply for onsite and offsite communications. This recommendation is being carried forward.
- to reducing the risk to operators in navigating to room 12701, the procedure will be updated to provide alternative means of directing operators to take certain routes from room 12351 to room 12701 during a station blackout (SBO).
- installing a seismically qualified connection flange to the PCCAWST to remove the need for operators to climb a ladder with a hose to gain access to a manway cover on top of the PCCAWST.

105. Both sets of analyses are enhanced by a comprehensive set of claims, arguments and evidence, which summarise the findings of the analysis.

106. Both activities are demonstrated to be relatively simple and straightforward – simple valves movements.

107. The time available is [redacted] (BDB-006) and [redacted] (BDB-005) respectively, while and the actual time needed to align valves etc. is a fraction of that. The dominant time factor in both analyses is the off-site response and site clean-up / restoration activities.

Some of the timing assumptions relating to the off-site response / clean-up activities may be optimistic so these will need to be validated during site-licensing.

108. I judge that the analysis of Beyond Design Basis Accident (BDBA) HBSCs is sufficient to close out CC-03 and contribute to the closure of GI-AP1000-HF-01.

109. Reference 24 also provides a summary of the wider provisions of technology, administrative, and welfare features designed to mitigate the effects of a BDBA.

110. Westinghouse recognised the importance of welfare and the psychological issues that are likely to arise during a BDBA and flagged these up to the future licensee. Accordingly, following feedback from ONR, it has produced a reasonable set of assumptions in this area for future Verification and Validation (V&V) during licensing. The assumptions include: the provision of potable water, comestible supplies, bedding and beds, availability of off-site persons and material / equipment, the use of Severe Accident Management Guidelines (SAMGs), the **AP1000®** BDB Long Term Coping Strategy and Conduct of Operations manual to aid decision-making.

111. Westinghouse set out assumptions regarding off and on-site response times. While these are helpful, I do not consider these to be particularly realistic given the transport infrastructure surrounding the local area where the **AP1000®** design will be sited. I also consider some of the durations assumed for clearing debris to be optimistic. However, as these are assumptions, and Westinghouse has declared that they will apply V&V to them a, these will be validated or corrected during site-licensing.

112. Westinghouse provided a credible set of arguments related to the technological features of the **AP1000®** design that minimise the need for human intervention following a BDBA. These arguments also describe the features that help minimise the risk of human error following the event. One example of this is a detailed summary of the communications systems available following the event to manage the incident – a key learning point from Fukushima.

113. Westinghouse described a number of reasonably practicable measures, which should serve to reduce the physical and psychological burden on the available personnel immediately after the event. For example, the permanent installation of cabling and hoses to minimise the need for operators to run-out long cable / hose runs.

114. Finally, Westinghouse has, as requested (Ref. 41) by ONR, provided an early definition of the staffing complement for the **AP1000®** design give an indication of how many people are likely to be available following a BDBA.

115. I judge that, given that GDA excludes specific siting hazards and organisational considerations – both will be considered during site licensing – Westinghouse has provided a sufficiently detailed assessment in the area of HF to close CC-03. This judgement is made with the following caveat: the exclusion of specific siting hazards and organisational considerations, renders some of the analysis presented somewhat artificial. This will need to be addressed by a future licensee during normal site licensing activities.

4.3.3 Phase 3 HEA

116. Following feedback from ONR that UKP-GW-GL-126 (Ref. 23) alone would not be sufficient to fully close out GDA issue GI-AP1000-HF-01, Westinghouse provided supplementary analysis in November / December 2016 in three areas. It enhanced the analysis of misdiagnosis and violation potential and re-assessed three of the HBSCs using a new and improved HEA method initially developed for use during licensing. This section describes my assessment of the HEA method and its application.

117. The method possesses the following attributes:

- a scenario overview describing the nature of the fault and the starting conditions, etc.;
- action description: a narrative description of the task/s being performed;
- assumptions applicable to the entire task: this section captures all the assumptions made about the task that will need future verification by the licensee;
- PSFs applicable to the entire task: a list of those PSFs that apply throughout the task;
- a Tabular Task, Time, and Error Analysis comprising the following headings:
  - Task number;
  - Cue / Plant Response: alarms, indications etc. relevant to the sub-task;
  - Person: who is performing the task;
  - Task descriptions;
  - Tools / Equipment / Interface items that the person interacts with during the sub-task;
  - Location where the task is performed;
  - Estimated time;
  - Cumulative time;
  - PSF influence specific to the subtask;
  - Error / Error Cause;
  - Consequence of failure;
  - Recovery opportunity;
  - Recommendations;
  - Assumptions; and
  - Notes
- drawings / Diagrams / Screenshots of the Tools / Equipment / Interface items that the person interacts with during task;
- [optional] failure path analysis;
- summary of the claims, arguments and evidence; and
- conclusions.

118. It follows the same staged approach as that used for the analysis presented in UKP-GW-GL-126 (Ref. 23).

119. Westinghouse has supplied three analyses of HBSCs using this method, one of each error type:

- Type A: OPR-011: Operators conduct testing and maintenance on the 14-inch automatic depressurisation system fourth stage squib valves;
- Type B: OPR-099: Operator executes the core make-up tank discharge valve operability test; and
- Type C: HEPO-FI-ADSDIS: Operator prevents fire-damage-related hot shorts from spuriously generating the signals necessary to actuate and open the automatic depressurisation system fourth stage squib valves.

120. I have assessed each of these in some detail and I discuss each in turn below, before providing an overall judgement on the adequacy to support the closure of GI-AP1000-HF-01 and its suitability for use during licensing.

OPR-011

121. OPR-011 is an HBSC relating to the testing and maintenance on the 14-inch automatic depressurisation system fourth stage squib valves. It was previously assessed in UKP-GW-GL-126 but found to have a number of analytical limitations.

122. This HBSC was re-analysed following an intervention by myself and mechanical engineering colleagues. We queried the achievability of the squib valve removal and maintenance tasks. We considered that the task design failed to reduce risks to ALARP. The task involved complex and precise winching and rigging activities to re-locate the valves to their maintenance positions. These were performed very close to safety critical pipe-work and components presenting a significant human performance challenge.

123. Following this intervention, Westinghouse carried out a design study and modified the task-design to minimise winching and rigging. The new method simply requires the valve to be moved axially to separate it from the associated pipe flange and it is then lowered onto its maintenance cradle. The reduction and simplification of valve movement significantly reduces the risk of damaging neighbouring safety critical systems, structures and components.

124. The HEA provides strong evidence that Westinghouse recognised the risk of Type A errors contributing to the latent failure of the valve. All squib valve designs incorporate mistake proofing principles (Poka Yoke). Examples include:

- Each tension bolt size is unique to each valve type precluding cross-fitting in error; only the correct bonnet, tension bolt, and piston can be used. Furthermore, the 8-inch bonnets have a mating ring that ensures they can only be assembled on the correct valve body.
- There are four Poka Yoke features incorporated into the cartridge design. Each cartridge has a different outer diameter (OD) and a different length. The smaller OD cartridge is the longest; so that even though it fits in the bonnet, the cartridge cover cannot be installed. The 8-inch valves have two initiators and the 14-inch valves have three initiators, therefore the cartridge cover cannot be installed. All the initiators are identical and isolated, so it does not matter which cable is attached to the initiator.
- Each shear cap is positioned within the valve body by bolts featuring a pitch circle diameter unique to the valve type. In addition, the valve body has specific tapped holes to suit specific shear caps. There are six Poka Yoke features incorporated in the shear cap design. On the flange of the shear cap for the 8-inch valve has two bolt holes where it mates with the valve body to align the shear cap to the body. The bolt-hole circle is different for each size of shear cap, so the shear caps cannot be installed in the wrong place. I also note that there are an additional ten bolt holes on the 8-inch valve to secure the shear cap to the body. The bolt-hole circle for these are the same on all 8-inch valves. The 8-inch high pressure (HP) valve, used for IRWST injection, has a left (-L) and right (-R) designation. This is to allow installation into the direct vessel injection rooms without the position indication switch interfering with the room walls. The differences are the direction of the flow arrow and the side on which the differently sized shear caps are installed.

125. I consider that the analysis substantiates the OPR-011 HBSC. It provides evidence that sub-tasks are achievable and contains sufficient detail on the sub task failure modes and also where recovery opportunities exist. It also identifies the most

important PSFs and makes recommendations for reasonably practicable to further reduce risk to ALARP.

126. The only limitation that I noted during my assessment, related to the omission of any analysis of the decision making associated with the detection of pyrotechnic cartridge damage (although it does flag up pyrotechnic damage as an error). A damaged pyrotechnic cartridge could result in the squib valve failing to actuate so I would have expected this to be covered, or a rationale provided for exclusion. Although this is a weakness in the analysis, it is not sufficient to prejudice the closure of GDA because:

- maintenance is planned to minimise common mode Type A errors, e.g. by planning maintenance regimes to avoid common cause failures; and
- the design of the ADS system features sufficient redundancy, so that one valve not available due to a Type A error would not prevent the safety system from functioning.

127. I am confident that this can be addressed during licensing and I will follow this up as part of normal regulatory business.

128. I judge that the revised HEA of OPR-011 has provided adequate evidence to justify the OPR-011 HBSC for GDA. I consider that any necessary additional analysis can be performed during licensing as part of the resolution of the Step 4 Assessment Finding:

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

OPR-099

129. OPR-099 is an operability test of the CMT isolation discharge valves. It can be performed at full-power or shutdown. Westinghouse's analysis considered the HBSC being performed at full-power as the consequence of interest is a Safeguards actuation and reactor scram. There are no time constraints in this task.

130. This HBSC is performed by four operators, supervised by the senior reactor operator who would be in the MCR at the time. The operators' tasks are as follows::

- one to perform the MCR based tasks;
- one e in the MCR for independent verification;
- one to perform the local actions at the PMS maintenance test panels and integrated logic control cabinets; and
- one local operator for independent verification.

131. To be successful, the operators have to correctly execute the CMT isolation discharge valves operability test. This includes closing the CMT inlet isolation valves PXS-V002 A/B, opening CMT discharge isolation valves PXS-V014 A/B and PXS-V015 A/B and returning the valves to their proper alignment.

132. Failure to close the CMT inlet isolation first and opening the CMT discharge isolation valves would result in an open flow path from the CMT into the RCS and the injection of highly boronated and cooler water into the reactor coolant – the boron concentration offsets any increases in cold water-addition caused reactivity. If this is not promptly identified and corrected, a Safeguards actuation and reactor trip occurs within approximately 3 to 5 minutes of the open flow.

133. Westinghouse has provided suitable and sufficient analysis including convincing evidence that it has assessed both the MCR and local panel aspects of the task. The analysis includes screenshots / panel photos of the HSI used to perform this task and I

consider that they provided clear information and controls to the operator. The job design appears robust, there are no time pressures associated with the task and there are opportunities for recovery from errors. MCR personnel monitor plant conditions specifically to detect that the plant response is as expected and there are two verifier roles associated with the task - one MCR based, the other local. The consequence of task failure is within the design basis. The analysis made a number of sensible recommendations aimed at further improving the opportunities for error detection. I consider that the HEA of this task substantiates the HBSC.

HEPO-FI-ADSDIS

134. HEPO-FI-ADSDIS is an HBSC in which the MCR has to detect and locate a fire in the ADS4 C&I cubicle of a single division of the PMS. A local operator is then dispatched who de-energises the cabinets in the affected division to prevent their spurious activation due to a hot-short. The squib valves are a component in one of the **AP1000®** design's emergency cooling systems. On spurious activation, they place the reactor into a large break loss of coolant accident (LOCA) which is a design basis fault and protected against; normally the system sequentially actuates valves ADS 1 through ADS4 to incrementally lower primary circuit pressure. Westinghouse has provided a safety case substantiating ADS4 actuation, without stages 1-3, at normal operating pressures. This HBSC is a defence-in-depth claim.

135. The scenario comprises the following:

- fire starts in PMS C&I cabinet ADS4 "arming" cabinet;
- fire is detected in the MCR;
- operators are dispatched to manually open the ADS4 circuit breakers to de-energise the affected division's PMS C&I cabinets before the fire spreads to adjacent ADS4 "Firing" cabinet via insulation material;
- based on the current fire analysis (Ref. 42) it would take a little over [redacted] minutes, from the outbreak of fire to possible squib valve actuation; and
- the PSA assumes [redacted] window of opportunity.

136. I consider that the HEA of this task demonstrated that it is relatively straightforward. The quality of the analysis is high. An issue was identified regarding the clarity of the fire detection process and this is reflected in this analysis. The limitation is being addressed as part of the HED resolution process. Breaker position indication is clearly indicated in the control room thus providing an independent check. [redacted]

137. Whilst I concur with Westinghouse's claim that the risk of incorrectly executing the task is reduced ALARP, I do not agree with the claim that it can be performed within the available time. This task has only [redacted] of contingency, which could be quickly eroded by unforeseen complications. Further, while this task is not a principal means of achieving a safety function, it does not meet the spirit of the following SAPs:

ERL.5	Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.
ESS.8	Automatic initiation	For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).
ESS.9	Time for human intervention	Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient.

138. In order to meet the PSA time window the operators must respond immediately. Westinghouse substantiated the impact of spurious activation of these valves. However, the consequence of their actuation, while mainly an operational inconvenience as it immediately places the plant out of action, will in the long run require a significant clean-up operation of primary circuit coolant, which in itself is a hazardous task.

139. I have discussed this with my colleagues (C&I, Fault Studies, PSA, and Mechanical Engineering) and an assessment finding is being raised in the Fire PSA Assessment Report which requires further ALARP analysis of this fault scenario and associated HBSC. In terms of the HEA assessment method, I have discussed this with Westinghouse and agreed that learning from this example will be taken forward in future assessments.

Conclusions

140. To conclude, I consider that the revised HEA method developed by Westinghouse provides suitable and sufficient analysis of HBSCs and took account of ONR's significant regulatory feedback. It explicitly addressed:

- the failure to link the task, error, PSFs and consequences cogently;
- the failure to adequately capture the analyst's insight on the page;
- the lack of explicit assumptions about the future operating organisation; and
- the lack of detail concerning how and why the human error might occur.

141. It has resulted in a methodology which I judge to meet GB best practice. My judgement is based on the fact that the analysis:

- clearly shows the relationship between: task, PSFs, consequences and recovery opportunities;
- provides cogent and coherent detail on all of the task factors (e.g. who, what, where, when and how);
- offers analyst insight into what errors can occur instead of listing all theoretically possible errors);
- suggests sensible ALARP recommendations;
- enhances reader understanding via the addition of diagrams, photos and HCI screen-shots; and
- provides temporal information when time is a critical factor to task success.

142. I consider it forms a sound basis for completion of further work to address the Step 4 assessment findings and future HEA during general licensing. I welcome that Westinghouse committed to updating or re-assessing existing analysis using this new analysis method and that these human error analyses will be provided as input into the probabilistic safety analyses during site Licensing.

4.3.4 Integrated System Validation Trials.

143. ISV trials are used to test and validate all of the HFE elements (training, procedures, human-technology interfaces, environment, staffing levels, etc.) that in concert, make up a human-systems interface. Their purpose is to test how each of these elements interact together and to either validate the system performance or identify limitations in any of the HFE elements. They are thus an effective HEA tool as they can and do show up adverse, complex interactions beyond the imagination of the analyst that lead to poor system performance.

144. Westinghouse's ISV trials tested the HSI of both the MCR and RSR over a wide range of plant states and faults. Further details of the trials and the scenarios can be found in Section 3.

145. The ISV trials largely met my expectations with respect to RGP for the following reasons:

- The **AP1000®** design ISV trials used a high fidelity simulation of the **AP1000®** design MCR and RSR.

- The trials employed SQEP operators supplied by US utility companies. They underwent training and assessment to qualify as licensed **AP1000®** PWR operators.

- The scope of the HBSCs tested was comprehensive. The performance of the HSI was evaluated across 23 complex scenarios ranging from normal to fault conditions. They showed that the MCR / RSR crew complete the following evolutions:
  - Heat up and start up the plant to 100% power;
  - Shut down and cool down the plant to cold shutdown;
  - Bring the plant to safe shutdown following the specified transients:
    - Reactor Trip
    - Turbine Trip
  - Bring the plant to a safe, stable state following the specified accidents:
    - Small-break LOCA;
    - Large-break LOCA;
    - Steam line break – Steam line and feed water breaks;
    - Feed water line break; and
    - Steam generator tube rupture.

146. Each of the 23 complex scenarios was undertaken a minimum of three times by three different crews. In the event of the success criteria not being met, a fourth run-through was performed. This provided repeated testing of the associated HBSCs.

147. To assess the coverage of HBSCs, I mapped the top-ten faults in the PSA plus two with lower significance to trials scenarios. These faults make up 87.6% of the total **AP1000®** design core damage frequency. It is possible to map a scenario to all but one of these faults indicating that, as a minimum, the trials assessed those HBSCs that make up 79.6% of total core damage frequency. The HBSC not covered relates to spurious IRWST recirculation injection and was the subject of a paper based analysis reported in Reference 23.

148. Table 5 shows the results of the mapping exercise, which gives confidence that all except one of the selected control room based HBSCs from the sample of 20 were tested. It is important to note that where some crews failed, this does not undermine the safety case. The purpose of ISV (and similar) trials is to rigorously test the full range of human-system performance to both, validate it and identify where issues exist.

149. Performance was assessed via; direct observation, post-hoc debriefs, cognitive workload analysis, situational awareness analysis, and questionnaires eliciting opinions on usability issues.
Where issues were identified, these were captured as HEDs to be ameliorated as part of the HED resolution process.

Table 5: Mapping of ISV Scenarios to Highest Core Damage Contribution Faults

Rank	Initiator	Frequency	% of CDF	Description	[redacted]
1	%SLOC	5.77E-08	33.00%	SMALL LOCA	[redacted]
2	%RVR	2.99E-08	17.10%	REACTOR VESSEL RUPTURE	[redacted]
3	%SPRECIRC	1.40E-08	8.00%	SPURIOUS IRWST RECIRCULATION INJECTION	[redacted]
4	%LOOP	1.30E-08	7.40%	TOTAL LOSS OF OFFSITE POWER	[redacted]
5	%SGTR	7.68E-09	4.40%	STEAM GENERATOR TUBE RUPTURE	[redacted]
6	%VWS	6.36E-09	3.60%	TOTAL LOSS OF VWS HCS	[redacted]
7	%LEAK	6.28E-09	3.60%	RCS LEAK	[redacted]
8	%SLBD	5.98E-09	3.40%	SLB DOWNSTREAM OF THE MSIVS	[redacted]
9	%SWS	4.31E-09	2.50%	TOTAL LOSS OF SERVICE WATER	[redacted]

Rank	Initiator	Frequency	% of CDF	Description	[redacted]
					[redacted]
10	%MVAC	3.89E-09	2.20%	LOSS OF MEDIUM VOLTAGE AC POWER	[redacted]
14	%SLBU	2.16E-09	1.20%	SLB UPSTREAM OF THE MSIVS	[redacted]
15	%FWLB	2.04E-09	1.20%	FEEDWATER LINE BREAK	[redacted]

150. I consider that the ISV trials provided an effective assessment of those HBSCs performed in the MCR and RSR. The trials provided robust evidence that the risk from human error has been reduced SFAIRP for this stage in the design process as it validates many of Westinghouse's HBSC claims and identified limitations in the HSI where some HBSC were invalidated. Those local-to-plant HBSCs included in the sample were analysed by Westinghouse in UKP-GW-GL-126 and the Phase 3 analysis. My assessment of these is discussed above in Subsections: 4.3.2. and 4.3.3.

151. Limitations, or HEDs, were identified from ~ 22,000 comment lines of raw data. These data were reviewed to organise, sort, and categorise them into comment groupings for further processing. A multi-disciplinary team consisting of representatives from HFE, procedures, training, simulators, and operations processed these groupings to identify the critical comments and issues. The data went through a number of iterations before they were synthesised into a list of 62 HEDs. These HEDs are currently being resolved prior to the re-testing of the MCR/RSR to validate that the HED solutions have addressed these deficiencies.

152. The trials complemented and enhanced the previous and current paper-based analysis and provided important data to improve the accuracy of the PSA. Westinghouse performed a PSA sensitivity study based on the findings of the trials. The trials data invalidated four existing HEPs and raised core damage frequency (CDF) by a factor 4, but this was still well below ONR's Base Safety Limit (BSL) (Ref. 43). Westinghouse has committed to utilising the output data from these and future trials in the PSA during the licensing period.

153. Minor limitations that I identified during my assessment comprise:

- The measure of cognitive workload used for the trials was a single aggregate score for each scenario. Workload profiles offer better diagnostic insight as they help identify discrete tasks with unacceptably high or low cognitive workload.
- 'Credible-but-bad-data' faults were not comprehensively tested. Westinghouse has committed to further testing in this area.
- Beyond design basis HSI performance was not comprehensively tested.

154. I consider that these limitations are sufficiently minor to not prejudice the closure of GF-AP1000-HF-01 or the granting of a DAC. They are also bounded by existing Step 4 assessment findings.

4.3.5 Assessment of Violation Potential

155. This section presents my assessment of Westinghouse's analysis of the potential for violation on the **AP1000®** design. It explains the concept of violation in the context of GDA, describes the scope of Westinghouse's submission and provides my judgement on its adequacy.

Definition

156. Violation can be defined as a deliberate non-compliance with rules or procedures. The key differentiator between violation and error is intent. In an error, a person is under the impression that they are compliant with the rule, procedure, or heuristic and is unaware of the deviation; there is no intent to make the error. In a violation, the act is deliberate.

157. The definition of violation can be further expanded to include:

- benign intent violations, e.g. someone cutting corners in the correct or erroneous belief that their actions are beneficial; and
- malicious intent violations, e.g. acts of vandalism or sabotage.

158. Acts of vandalism or sabotage are outside of the scope of my assessment.

159. ONR's formal position on the assessment of violation by a licensee or requesting party is described in TAG-061 Human Reliability (Ref. 7). It guides ONR inspectors to consider whether:

160. *"The process of task analysis has been used to qualitatively identify and model foreseeable violations and demonstrate the adequacy of any plant and organisational factors that are claimed to minimise violation producing conditions. It is not, however, a current expectation that foreseeable violations are identified and quantitatively modelled in the safety case due to limitations in the sophistication of current HRA techniques to quantify such events*."

Scope of Submission

161. Westinghouse's substantiation of violation behaviour underwent a number of iterations, taking into account ONR's feedback. The final iteration (Ref. 27) attempted to:

- provide sufficient substantiation that the design features of the **AP1000®** design can reduce violation behaviour ALARP; and
- summarise Westinghouse's assumptions regarding the future licensee operation of the plant.

162. The submission sets out Westinghouse's assumptions about future operation in the following areas:

- nuclear safety culture;
- reactor operator training and qualification; and
- conduct of operations.

163. It also attempted to demonstrate that those areas within the scope of GDA reduce violation potential ALARP:

- HSI design features;
- cognitive error assessments; and
- local-panels and maintainability HF engineering assessment.

164. Finally, it presented an overview of where future work is needed, including commitments against these needs. Identified future packages of work are to:

- validate, with the site licensee, assumptions relating to minimising violation behaviour;
- complete ISV trials on a GB **AP1000®** PWR simulator to include C&I and HSI software failures;
- complete and document the HED resolution and re-verification/re-validation process;
- complete detailed cognitive HEA for risk significant human actions, including maintenance and removal of ADS squib valves, to serve as human reliability analysis input to the future PSA updates; and
- complete the local panel and maintainability HF assessments.

Nuclear Safety Culture

165. Safety culture is out of scope for GDA. Westinghouse sensibly sets out an assumption that the GB **AP1000®** design will be operated in line with current US RGP - Institute of Nuclear Power Operations (INPO) guidance, or equivalent, in the areas of leadership, organisation and safety culture. I consider this to be an appropriate assumption at this stage.

Reactor Operator Training and Qualification

166. Operator training and qualification is also out of scope for GDA; Westinghouse assumed that any reactor training and qualification programme set up by the future licensee would be based on the IAEA Systematic Approach to Training (SAT) method. This approach is recognised as RGP in GB; it is the basis of ONR's own inspector guidance on this topic. I am content that this is a sound basis for developing the future **AP1000®** PWR training programme.

Conduct of Operations

167. Conduct of Operations (CoO) is also out of scope for GDA. Westinghouse assumes that the same basic CoO model used in the US will be used in GB. This model benefits from feedback from the domestic US utility base and has been developed over a number of years. It clearly articulates the roles, responsibilities, and behaviours for those staff with an important safety role; Westinghouse provided CoO examples where violation behaviours could be mitigated. I was able to witness a practical demonstration of the **AP1000®** PWR CoO during an inspection of Westinghouse in October 2016 (Ref. 44). During which I spent two days in the **AP1000®** PWR simulator observing a number of simulated plant evolutions. The conduct of operations I observed during this time was excellent. Communications were clear and a clear control hierarchy was observed, yet there was an open and questioning attitude displayed by all. Judged against the principles of good crew resource management (CRM), which aim to enhance situational awareness, self-awareness, leadership, assertiveness, decision making, flexibility, adaptability, event and mission analysis, and communication, the Westinghouse CoO appeared to support each of these characteristics. I consider that Westinghouse has provided a sufficiently robust argument that the CoO model should contribute to the reduction of violation behaviour ALARP.

HSI Design Features

168. Poorly designed technology, which lacks affordance (the properties of an object or system that define its possible use or make clear how it can or should be used) or ignores the principles of usability, can lead to the increased likelihood of violation behaviour as users seek to self-optimise their interactions with it. Westinghouse's

submission articulated the rigorous design process that the MCR and RSR have undergone. It explained how operational experience from Westinghouse customer utilities has been factored into the design and presents a number of examples that should specifically reduce the potential for violation. For example, the response to unusual plant conditions, which require knowledge-based reasoning, can be particularly error prone or subject to non-compliance with procedures. The **AP1000®** design mitigates this by the addition of function based displays, which are supported by accompanying procedures. These reduce the need to act outside the procedure as they specifically address the problem of unanticipated events that do not entirely match a procedural response.

169. Westinghouse also has specifically addressed the problem of failing to comply with procedures by adopting task-based displays. These draw together the required functionality onto (where practical) a single page thus removing the need for navigation between multiple pages; the greater the number of navigation steps to acquire data, the greater the chance that checks will be deliberately omitted because of the effort involved. The submission presented other examples including the use of design features limiting single person actuation of some risk-important activities.

170. It is clear that Westinghouse has specifically considered the need to optimise operator interactions with the key HSIs in the **AP1000®** design, which will help to minimise the likelihood of violation behaviour.

171. It is also possible to draw confidence that violation potential has been minimised from the ISV trials. Westinghouse specifically highlights three violations (over 23 scenarios tested) that were observed during the trials. These included: a switch issue, in which it was unclear to the operators that it needed to be returned to a neutral position so they failed to do so; a potentially unclear procedure response; and an issue with the number of alarms presented during transient conditions. None of these issues is sufficient to hold up GDA and I consider them typical of the development and testing process of complex interfaces. Westinghouse is currently working on solutions to these HEDs and will be testing solutions during future domestic US ISV trials. It has also committed to a set of GB specific trials during site licensing.

Cognitive Error Assessments

172. Westinghouse acknowledges the previous limitations in its paper based HEA with respect to detecting violation potential. It has committed to performing further work in this area during licensing. I do not consider this to be a concern as the key violation driver at this stage of the GDA / licensing programme is design induced violations and Westinghouse has provided sufficiently robust evidence in this area.

Local Panels and Maintainability HF Engineering Assessment

173. While Westinghouse has gone some way to optimise local panel and maintenance interactions via the use of design guides, and some maintainability studies, there is evidence (Ref. 44) that this is not up to the same standard as that applied to the MCR / RSR.

174. During my October 2016 inspection (Ref. 44), I observed the proposed methodology for removing the ADS squib valves for maintenance. It was clear that the task design did not optimise human performance. Westinghouse responded to feedback at the time, and it has now completely revised the task to optimise it. The optimisation process was supported by detailed HEA (Ref. 28). It is also encouraging that Westinghouse acknowledged in this submission that this area that will need further work during licensing. The proposed scope of this work comprised the following:

- risk-significant systems, structures and components identified in Reference 45;

- local components involved in EOPs;
- components / tasks associated with potential maintenance errors;
- rad-waste control room and rad-waste local station, including local Ovation™ stations;
- electrical systems, e.g., electrical rooms, motor control centres (MCCs);
- C&I cabinets, e.g., component interface module ; and
- other local plant control stations and equipment as per the HF engineering program on case-by case basis, (e.g., programmed and remote systems, fuel handling equipment, and cranes, DCPs).

175. While there are limitations in the optimisation of local to plant tasks, I consider that Westinghouse has provided sufficient cogent evidence for me to conclude that all the important for safety plant HSIs can be optimised prior to critical operation of the **AP1000®** design.

Conclusion

176. The basis of my assessment of Westinghouse's violation submission is informed as follows:

- The violation factors relevant to GDA are predominantly those that fall within the technology and task-design category. These have been comprehensively addressed through the HSI design and trials processes.
- Violation factors pertaining to the operating organisation are specifically excluded from the GDA process. These will be considered in detail during the licensing of the **AP1000®** PWR and I found that Westinghouse has captured any assumptions important to safety relating to the operating organisation.
- The **AP1000®** design is still not completely finalised. For example, the MCR, where the majority of the HBSCs are performed, remains subject to a large number of HEDs that are currently being addressed by Westinghouse's HED resolution process. This resolution process supports a range of improvements, including minimising the potential for violations.

177. Westinghouse has focused attention on providing a sensible set of assumptions about those factors outside the scope of GDA and on analysing the technological and task design features that could contribute to an increased risk of violation potential. I consider that it has achieved both these goals and has submitted an analysis of violation potential appropriate for GDA. I judge that Westinghouse has provided compelling holistic evidence, supported by a reasonable set of assumptions, that violation behaviour can be reduced ALARP on the **AP1000®** design.

4.3.6 Assessment of Misdiagnosis Potential

178. This section presents my assessment of Westinghouse's analysis of the potential for misdiagnosis on the **AP1000®** design. It explains the concept of misdiagnosis in the context of GDA, describes the scope of Westinghouse's submission, and provides my judgement on its adequacy.

Definition

179. Misdiagnosis occurs where symptoms are insufficiently distinct from one another to draw a clear diagnosis. It can also occur due to a basic lack of understanding as a result of poor training. As training is firmly within the scope of site licensing, my assessment has focused on whether Westinghouse has provided a cogent and coherent design and safety case where misdiagnosis can be reduced ALARP.

180. There are a number of ways in which misdiagnosis potential can be analysed, including:

- confusion matrix analysis. A method whereby fault symptoms are compared with other fault systems to identify similarities;
- HEA: the potential for misdiagnosis can be considered as part of a wider HEA; and
- simulation studies: using simulators to run through multiple scenarios and evolutions and observing whether fault diagnosis is reliable.

181. ONR does not specify a particular method; each has its pros and cons within the design and safety analysis process. Indeed, Westinghouse's submission drew together multiple work streams to present the case.

182. Westinghouse's substantiation of misdiagnosis underwent a number of iterations, taking into account ONR's feedback. The final iteration sought to:

- provide a multi-legged substantiation that the **AP1000®** design reduce misdiagnosis potential ALARP; and
- summarise Westinghouse's assumptions about the future licensee operation of the plant.

183. The submission presents claims, arguments, and evidence from the following Westinghouse work streams:

- Operating Experience Reviews (OpEx) reviews;
- task analysis and HF task support verification;
- HF/HSI design guidelines and HF design verification;
- HF ISV;
- HED resolution process;
- plant procedure development;
- HSI design features; and
- CoO

Operating Experience Reviews

184. Westinghouse performed a comprehensive OpEx review (Ref 46) of the US domestic civil nuclear industry. This review included data from NRC event bulletins, circulars, information notices, etc. It also included data from the Westinghouse Owners Group. This scope provided learning from Westinghouse PWRs, non-Westinghouse PWRs, and boiling water reactors. It also included some learning from other high-hazard sectors where technological parallels could be drawn. This was used to inform the HSI design to avoid previously identified misdiagnosis issues.

Task Analysis and HF Task Support Verification

185. One of the objectives of Westinghouse's task analysis and HF task support verification programme was to identify all the controls and indications needed to permit reliable operation of the **AP1000®** design including fault diagnosis. This programme has been shown to be successful (Ref. 47) as almost all HEDs identified during the ISV trials relate to the method of presentation rather than the omission of data or controls. This gives confidence in the adequacy of the task information provided to support fault diagnosis.

HF/HSI Design Guidelines and HF Design Verification

186. Westinghouse followed HF/HSI guidelines (Ref. 48) during the development of the **AP1000®** design. These guidelines are based on US industry RGP and US NRC requirements. The output was subsequently subject to a design verification activity to ensure that the guidance had been followed. Evidence of this process was reported in the **AP1000®** design HFE Design Verification Report (Ref. 49) along with the discrepancies identified. These were captured as HEDs for future resolution.

HF ISV / HED Resolution Process

187. I am able to draw significant confidence from Westinghouse's simulator trials of the **AP1000®** design. Predictive misdiagnosis analysis, whilst a useful tool early in the design process, is constrained by the limitations of the psychological understanding of human complex-system interactions, and the limitations of the analyst to postulate every failure. The benefit of simulation-based analysis is that it provides an opportunity to test in real-time, in concert, all the various HSI elements. It also allows complex inter-operator interactions to be analysed and the way in which various HSI elements either support or hinder this process. Finally, they provide strong evidence of whether the design reduces human error / misdiagnosis ALARP. I consider the Westinghouse **AP1000®** design ISV trials to have achieved this. As could be expected of a complex HSI, the trials identified five HEDs (Ref. 25) relating to misdiagnosis. However, the trials showed that "*the respective plant operations were capable of being performed; necessary tasks were completed such that the health and safety of the public would not be challenged, and that the integrated system supported the safe operation of the plant.*" (Ref. 25)

188. While I consider the Westinghouse ISV trials were a competent and rigorous analysis of the HSI, I do not believe that they adequately considered credible-but-bad-data faults. This is because they were a product of the US **AP1000®** design licensing process and were never intended to be used as part of the **AP1000®** design GB safety case. 'Credible-but- bad-data' failure types are a likely source of misdiagnosis and I discussed this omission with Westinghouse in October 2016 (Ref. 44). I therefore draw further confidence from the subsequent Westinghouse commitment to carry out a set of GB specific simulator trials which will include the analysis of credible-but-bad-data faults. The full scope of the GB trials will include the analysis of:

- GB specific design changes from the standard **AP1000®** design;
- C&I and HSI resource software failures (e.g. failure of displays to update, failure of alarm system to update); and
- further validation of PSA time window s associated with the HBSCs that will be identified from the PSA updates to be completed during site licensing.

Plant Procedure Development

189. The US Three Mile Island (TMI) nuclear incident, which was in part caused by manifold diagnostic failures, served as a catalyst for a significant programme of research and analysis focus on the optimisation of plant procedures. The goal of this effort was to minimise the occurrence of future diagnostic errors within the industry. This work has continued since the incident in 1979 and Westinghouse claim that the **AP1000®** design benefits from the sum of this work; ~ 30 years of operating experience from more than 100 Westinghouse PWRs.

190. During my inspection (Ref. 44) I was able to observe the culmination of this effort to minimise diagnostic error. The system works as follows. The Emergency Operating Procedure (EOP) network is made up of two discrete procedure types. Optimal Recovery Procedures (ORPs) and Functional Restoration Procedures (FRPs). Different elements of the HSI have been specifically developed to support the use of both of these procedure types.

191. Upon receipt of a reactor trip or Safeguards actuation signal, the crew enter the relevant ORP. This guides the crew on a step-wise assessment of plant symptoms to diagnose the cause. It then advises the solution to put the plant into a safe-stable-state.

192. However, should the crew erroneously diagnose the fault and initiate a recovery plan that could hazard the plant, the FRPs come into play. The FRPs are used in concert with the permanently displayed Critical Safety Function (CSF) Wide Panel Information System (WPIS) page. The CSF page displays the six critical safety parameters in order of importance for nuclear safety – the order automatically changes in response to plant state. These include reactivity control, heatsink status, inventory, etc. Their 'health' is indicated by colour coding: Green = Healthy; Yellow = not-met; Orange = significantly challenged; Red = Severely Challenged. Should any of the CSFs become challenged (significantly or severely) then then operators must leave the current ORP and select the appropriate FRP based on the CSF and the severity of the challenge. Monitoring the CSFs is performed by the Shift Technical Advisor.

193. Thus, in the event that the crew attempt to hazard the plant in response to a misdiagnosis, they are warned of this as the relevant CSF changes status. The CoO mandates that in the event of a challenged CSF, the crew must stop what they are doing and engage with the relevant FRP. These essentially guide the crew to re-evaluate the previous diagnosis. I observed this system in practice during my October 2016 inspection and it appeared to work very well as a method of detecting misdiagnosis errors. This gives confidence that should misdiagnosis occur, the system supports and guides recovery from it.

HSI Design Features

194. Westinghouse claimed other HSI design features as protection against misdiagnosis errors. These include:

- Automatic status detection of plant parameters to indicate the completeness of procedural steps within the computerised procedure system. Bringing this information together reduces the risk of missing critical information and thus forming the wrong mental model.
- Automatic surveillance of data monitored in parallel with the execution of the main procedural steps. Critical changes in these data are automatically indicated to the operator, again reducing the risk of missing diagnostic differentiators.
- Suggested follow on procedures based on indicated plant symptoms. This feature moves some of the decision making from the operator, where time may be a factor,

to the design team where time is not, thus reducing the risk of selecting the wrong course of action.
- The WPIS, which provides an overview of the CSFs, alarms, and the primary, secondary, and balance of plant parameters to support shared understanding of the situation.

195. Should these systems fail, then the **AP1000®** design still benefits from the ~3000 plant years of paper-based procedure development.

Conduct of Operations

196. Westinghouse claimed that its CoO contributes to minimising diagnostic error. During my October 2016 inspection, I spent two days in the simulator observing a crew working through a number of normal and abnormal evolutions. During this time, I compared the crew's performance (CoO) against what I would expect if the principles of CRM were being followed – effective CRM has been shown to reduce the risk of misdiagnosis within the aerospace sector. What I observed did indeed meet these expectations. There was evidence of a clear control hierarchy; workload was effectively balanced between the crew; peer checking was in evidence; at relevant points during the evolution, the senior reactor operator sought active conformation that all parties concurred on the next course of action; and briefings were provided frequently to maintain a shared situational awareness and made good use of the WPIS resource. Overall, I judge that Westinghouse's claim that its model for conduct should help reduce diagnostic error ALARP is valid.

Conclusions

197. Based on my assessment of the misdiagnosis submission (Ref. 26), I consider that Westinghouse provided a range of suitable and sufficient information to allow me to conclude that misdiagnosis potential can be reduced SFAIRP on the **AP1000®** design.

198. Westinghouse has committed to the following activities during licensing:

- ISV trials on the GB **AP1000®** PWR simulator to include C&I and HSI software failures;
- completion and documentation of the HED resolution process (for both standard and GB plants);
- Completion of detailed cognitive HEA for risk significant human actions to serve as HRA input to the future PSA updates; and
- conversion of the standard **AP1000®** PWR plant procedures, including CoO), to GB **AP1000®** design site specific procedure, supported by an appropriate procedure V&V exercise.

199. This will further extend the work to minimise the potential for misdiagnosis and I judge that Westinghouse has provided sufficient material to recommend closure of this part of GI-AP1000-HF-01.

4.3.7 HEA Conclusions

200. Drawing across the work on HEA, violations and misdiagnosis it is clear that Westinghouse has submitted a broad body of evidence in relation to HEA

201. Westinghouse initially submitted a significant quantity of paper based HEA which, while having some value, did not sufficiently meet regulatory expectations in the scope and depth of analysis. This analysis did however provide a valuable basis for discussion, including consideration of misdiagnosis and the potential for violations.

202. From this dialogue Westinghouse built on and extended the original analysis to develop an iteration of the paper based HEA method. I have reviewed this approach and consider it to be consistent with GB best practice. I note that the analysis performed using this method, while currently limited in its extent of application, provides confidence that future HEA work undertaken to address the extant Step 4 assessment findings will be of good quality. I further note and welcome that Westinghouse committed to updating or re-assessing existing analysis using this new analysis method and that these human error analyses will be provided as input into the probabilistic safety analyses during site licensing.

4.4 Vulnerability of the AP1000® PWR Design to Human Error

203. Current generation PWR power stations typically present a core damage frequency of the order of 2 x 10-3 without taking credit for HBSC and 3.9 x 10-5 with credit (Ref. 33). In contrast, the **AP1000®** design claims a significant improvement in the human contribution to risk.

204. Westinghouse submitted a sensitivity study (Ref. 30) of the internal events at-power PSA, which showed that, if all HBSCs fail, the core damage frequency increases by x100 to 1.8E-05/year. This is well within ONR's Target 8 - BSL of 1E-4/year when credit for containment is considered at 0.1/demand. Target 8 is for an off-site dose greater than 1000 mSv.

205. When full credit is taken for containment, the frequency of an off-site dose greater than 1000mSv reduces to 1E-6/year, or around the Base Safety Objective (BSO).

206. Although the PSA is sensitive to human error by a factor of 100, the ONR BSL is still met and risks below the BSO could be expected once realistic human failure rates are used. This provides confidence that the basic allocation of function and task design within **AP1000®** design is sound. This does not negate the need for proper substantiation of HBSC but it does provide evidence for the closure of GI-AP1000-HF-01.

207. While my expectation is that Westinghouse will develop a complete and credible HF safety case, with adequate demonstration of the safety claims and requirements on the human actions, this analysis gives confidence that the **AP1000®** design is relatively insensitive to degradation in performance of the HBSCs.

4.5 Assessment Findings

208. During my assessment, five candidate assessment findings were identified. These comprised the following. Appended to each is the existing Step 4 assessment findings which bound them.

- The measure of cognitive workload used for each trials scenario was a single aggregate score. Workload profiles offer greater diagnostic insight as they show peaks and troughs, which reveals those subtasks where cognitive workload may be unacceptably high or low. Profiles are considered to be RGP.
  AF-AP1000-HF-41 - The licensee shall justify or redevelop the scope of the Westinghouse proposals for V&V and ISV.

- Credible-but-bad-data faults were not comprehensively tested. These faults have the potential to cause diagnostic error. Westinghouse has committed to further testing in this area.
  AF-AP1000-HF-41 - The licensee shall justify or redevelop the scope of the Westinghouse proposals for V&V and ISV.

- Beyond design basis human-system performance was not comprehensively tested. It has previously been assessed using walk-throughs and scripted role play. Following Fukushima, beyond design basis simulation has started to be adopted as it offers greater accuracy when assessing human-system performance.
  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.

- The ADS4 squib valves maintenance analysis failed to analyse the decision making associated with the detection of pyrotechnic cartridge damage (it does flag up pyrotechnic damage as an error). A damaged pyrotechnic cartridge could result in the squib valve failing to actuate.
  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.

- The task-design for the maintenance of squib-valves and the lack of HFI into COTS equipment both indicate that further HFI into the design of local systems, structure and components is required.
  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®.

209. However, in reviewing the previous Step 4 assessment findings, which Westinghouse is already required to address moving forward, I am confident that these bound the candidate findings above and should ensure that they are adequately addressed. Therefore, I do not raise any additional assessment findings but will instead monitor progress on the candidate issues as part of the existing Step 4 issues during licensing.

210. These matters do not undermine the generic safety submission and are primarily concerned with the provision of site specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. These items are captured as assessment findings.

211. Residual matters are recorded as assessment findings if one or more of the following apply:

- site specific information is required to resolve this matter;
- the way to resolve this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters; and
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

5 CONCLUSIONS

5.1 Human Factors Integration

212. In general I have found that Westinghouse applied itself to the integration of HF and that its processes now adequately support the identification and analysis of HBSCs. In particular I note that Westinghouse expanded its scope of identification by assessing all 51 GDA issues for additional previously unidentified HBSCs. Westinghouse has also proportionally reviewed all DCPs and identified additional previously unidentified HBSCs. This gives confidence in the rigour and completeness of the HBSC identification.

213. I found that HBSCs are managed via Westinghouse's HAD and I am content with Westinghouse's method for selecting HBSCs from the human action database for further detailed analysis and substantiation. I have reviewed the method and underpinning criteria and judge that it combines risk and representation to inform the selection of HBSCs. I consider this to be a sensible and proportionate approach.

214. In addressing this issue I note that Westinghouse responded constructively to challenges made by ONR and has put considerable time and effort into the development of its expertise in this area. As a result of this, it is my view that it has developed a credible and responsive HF design and analysis capability. This is important in supporting the effective deployment of HFI, the reliable identification of HBSCs and ultimately in supporting the licensing of the AP1000 ® design.

5.2 Human Error Analysis

215. From my review of Westinghouse's HEA, it is clear that there has been a number of challenges in the development of a cogent and coherent HF Safety Case for **AP1000®** design. Westinghouse has, however, persevered in applying itself to the issues raised and, in doing so, has ultimately brought together a strong set of supporting evidence, as detailed below.

- Westinghouse initially submitted a significant quantity of paper based HEA which, while having some value, did not sufficiently meet regulatory expectations with regard to its scope and depth of analysis. This analysis did however provide a valuable basis for discussion, including consideration of misdiagnosis and the potential for violations. From this dialogue Westinghouse has built on and extended its original analysis to develop a revised iteration of the paper based human error method. I have reviewed this approach and consider it to be consistent with GB best practice. I note that the analysis performed using this method, while currently limited in its extent of application, provides confidence that future HEA work undertaken to address the extant Step 4 assessment findings will be of good quality. I further note and welcome that Westinghouse has committed to updating or re-assessing existing analysis using this new analysis method and that these human error analyses will be provided as input into the probabilistic safety analyses during site licensing.

- In addition to the paper based analyses Westinghouse has also presented credible evidence relating to the substantiation of operator actions from its ISV trials. These have comprised a thorough analysis of the human system performance of the MCR and RSR. This analysis addresses the majority of HBSCs associated with normal operations and faults that contribute to core damage. I have found that the trials provided a valuable opportunity to evaluate the HBSCs and to scrutinise associated errors and that, in effect, the range and depth of analysis undertaken by Westinghouse substantiates the majority of HBSCs. In addition, where HBSCs have not been substantiated through the trials, the root causes have been identified and solutions are currently being progressed. Westinghouse has also

committed to verifying and validating these solutions during further planned trials. I consider this to be strong supporting evidence in relation to the substantiation of HBSCs and note that the trials have also promoted holistic consideration of both diagnostic error and the potential for violation.

- In addition to the submission provided by Westinghouse, I have observed a number of scenarios which contain HBSCs in the **AP1000®** design MCR simulator. From my observations I consider that the C&I is well laid out, presenting clear and unambiguous information to the operators. Noting the artificiality of a simulation, the crew were reliably able to detect and diagnose plant faults and respond in a timely manner. Intra-crew communications reflected RGP and the crew demonstrated a high level of shared situational awareness. I further note that the conduct of operations worked well, as did the procedures.

5.3 Risk Sensitivity of the Design and Safety Analyses to the HBSCs

216. My assessment found that the **AP1000®** design places only limited reliance on the HBSCs to remain within target safety limits. In particular I note that the extant at-power PSA shows that if all HBSCs fail (human error probabilities are set to 1.0), the core damage frequency increases by a factor of 100 and moves to 1.8E-05/year. When credit for containment is considered at 0.1/demand, this is well within the ONR Target 8 BSL of 1E-4/year and gives confidence that safety targets will be achieved. (Target 8 is for an off-site dose greater than 1000 mSv)

217. With full credit for containment, the frequency of an off-site dose greater than 1000mSv is around the BSO of 1E-6/year. While taking no credit for human actions within the PSA is sensitive, based on Westinghouse's analysis, I judge that ONR BSLs can be met and risks below BSOs would be expected once containment is considered and realistic human failure rates are used within the probabilistic risk model.

218. While my expectation is that Westinghouse develop a complete and credible HF Safety Case, with adequate demonstration of the safety claims and requirements on the human actions, this analysis gives confidence that the **AP1000®** design is relatively insensitive to degradation in performance of the HBSCs.

5.4 Overall Conclusions

219. Overall, Westinghouse has undertaken a significant volume of HF assessment in addressing this GDA issue and has applied considerable competent HF resource. I note in particular the strength and depth of evidence to substantiate the HBSCs provided by Westinghouse's ISV trials, and the recent iteration of its paper-based human error method which I consider to be consistent with GB best practice.

220. Based on the review of this evidence, it is my view that Westinghouse's submissions, when viewed holistically, identify, analyse and substantiate the key HBSCs SFAIRP for GDA. I have also identified no sufficiently significant safety issues in the area of HF that could prejudice construction of the **AP1000®** PWR in GB.

221. I further note that Westinghouse has provided compelling holistic evidence, supported by a reasonable set of assumptions, that both diagnostic errors and the potential for violation can be reduced to ALARP on the APP 1000 design.

222. I therefore recommend the closure of GI-AP1000-HF-01.

6 REFERENCES

1. GI-AP1000-HF-01 Completeness of the HF Safety Case, http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-hf-01.pdf
2. Westinghouse UK – AP1000 Generic Design Assessment – Resolution Plan for GI-AP1000-HF-01 – Completeness of the Human Factors Safety Case – Rev. 3. https://www.google.co.uk/search?q=AP1000+GDA+HF-01&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe_rd=cr&ei=Ir3TWKaxE9ST8QfFzp7wCw
3. ONR Guidance on Mechanics of Assessment, TRIM 2013/204124
4. GDA Guidance to Requesting Parties, www.onr.org.uk/new-reactors/ngn03.pdf
5. The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051 Revision 4, www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf
6. Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014, www.onr.org.uk/saps/saps2014.pdf
7. ONR Technical Assessment Guides http://www.onr.org.uk/tagsrevision.htm
8. GI-AP1000-CC-03 Consider and action plans to address the lessons learnt from the Fukushima event. http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-03.pdf
9. GI-AP1000-ME-01 Squib valve concept and design substantiation. http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-me-01.pdf
10. GI-AP1000-PSA-02 Fire PSA. http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-psa-02.pdf
11. UKP-GW-GL-042, United Kingdom AP1000 Human Factors Program and Assessment for the United Kingdom revision 0
12. UKP-GW-GL-793 - United Kingdom AP1000 Pre-Construction Safety Report – Chapter 13 Human Factors – Rev 0D
13. 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
14. UKP-GW-GL-070, Rev. 0, United Kingdom AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA.
15. 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
16. UKP-GW-GL-072, Rev. 0, United Kingdom AP1000 - Supplemental Information for the UK AP1000 Human Factors Safety Case – Potential Improvements As Proposed in the ALARP Analysis.
17. 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.
18. UKP-GW-GL-074, Rev. 0, United Kingdom AP1000 - Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability
19. UKP-GW-GL-075, Rev. 0, United Kingdom AP1000 - Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults.
20. UKP-GW-GL-076, Rev. 0, United Kingdom AP1000 - Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms.
21. RQ-1293 Substantiation of Actions Important For Safety – 27th October 2014
22. RQ-1294 Scope of ONR Human Factors Assessment – 27th October 2014
23. UKP-GW-GL-126 – Revision 0 - United Kingdom AP1000 Human Factors Qualitative Error Analysis.
24. UKP-GW-GGR-201 – Revisions 1 – United Kingdom AP1000 - Plant Post-Fukushima Assessment

25. APP-OCS-GER-320 Rev 0 Sept 2015 AP1000 Human Factors Engineering Integrated System Validation Report
26. WEC-REG-1432N – (NPP_JNE_001432) -Enclosure 1 – Misdiagnosis Potential
27. WEC-REG-1432N – (NPP_JNE_001432) – Enclosure 2 – Violation Potential
28. WEC-REG-1477N – (NPP_JNE_001477) – Enclosure 1 – Revised Human Error Analysis
29. WEC00025N – APP-GW-005-Rev-0 - Safe and Simple – The Genesis and Process of the AP1000 Design – 2008
30. APP-PRA-GSC-322- Rev B – AP1000 Plant At-Power Internal Events PRA Quantification Notebook
31. Not used.
32. NS-PER-GD-014, Purpose and Scope of Permissioning
33. 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 http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-hf-onr-gda-ar-11-012-r-rev-0.pdf
34. RQ-AP1000-1361 – Integration of HF / PSA and Fault Studies Disciplines – 8th July 2015
35. RQ-AP1000-1361 – Integration of HF / PSA and Fault Studies Disciplines – 27th August 2015 – Full Response
36. RQ-AP1000-1308 – Scope and Detail of Human Error Analysis – 11 February 2015
37. RQ-AP1000-1598 – Further Information Required on WEC GDA Issue Review – 22 August 2016 – Full Response
38. Westinghouse-REG-000737N - (NPP_JNE_000737) – Enclosure 1 – Status of ongoing HFI across GDA Issues
39. Westinghouse Report UKP-GW-GL-116, Rev 0, United Kingdom AP1000 - AP1000 Supplemental Information for the Human Factors Safety Case – Review of Selected Design Change Proposals included in the 2015 Design Reference Point for GDA," September 2015.)
40. NUREG-2114, Cognitive Basis for Human Reliability Analysis, U.S. Nuclear Regulatory Commission
41. RQ-AP1000-1485 – GDA Issue CC-03 Report UKP-GW-GGR-201 Review Comments – Human Factors – 5th February 2016
42. AP1000 PMS/DAS Cabinet Fire Analysis – APP-GW-AFR-001, Rev 0, June 2016
43. RQ-AP1000-1721 – Impact of Revision to HEPs following ISV Trials and Further WEC Qualitative HF Analysis – 14th October 2016.
44. ONR-NR-CR-16-724 – ONR Information Gathering Inspection at WEC Cranberry – 25-27th October 2016.
45. APP-GW- GL-011, AP1000® Identification of Critical Human Actions and Risk Important Tasks
46. APP-OCS-GJR-001 Human Factors Engineering Operating Experience Review For The AP1000 Nuclear Power Plant, May 2006
47. APP-OCS-GER-220 AP1000 Human Factors Engineering Task Support Verification Summary Report, June 2016
48. APP-OCS-J1-002, Rev 5, AP1000 Human Systems Interfaces Design Guidelines.
49. APP-OCS-GER120 AP1000 HFE Design Verification Report

Annex 1: Screening Criteria for HBSC sample and HBSC listing

223. Westinghouse proposed the following criteria for selecting human actions for further assessment during Step 4; they were agreed by ONR as appropriate. They are based on:

- Risk Achievement Worth (RAW), which is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk with the event failed to the baseline risk level.
- Risk Reduction Worth (RRW), which is the decrease in risk if the feature is assumed to be perfectly reliable. It is expressed in terms of the ratio of the baseline risk level to the risk with the feature guaranteed to succeed.

224. The criteria that Westinghouse used to establish risk important actions comprise:

- A human action is considered risk-important if the CDF or LRF increase is 200%, i.e. the RAW is ≥ 3.0. For the "focused" PRA study (with assumed failure of non-class 1 mitigating features), a human action is considered risk-important if the percentage increase is 100%, i.e. the RAW is ≥ 2.0. Any value below these criteria is considered to be not risk-important.

- A human action is considered risk-important if the CDF or LRF decreases by more than 10%, i.e. the RRW is ≥ 1.1. For the "focused" PRA study (with assumed failure of non-safety mitigating features), a human action is considered risk-important if the percentage decrease is 5%, i.e. the RRW is ≥ 1.05. Any value below these criteria is considered to be not risk-important.

- Qualitative factors are also considered:
  - If the RAW / RRW values are less than but close to the criteria and the time available for the operator to act is close to the available time.
  - The actions are complex, unique, or potentially challenging.
  - The actions are needed to prevent conflicting safety goals.
  - Actions that are judged to be risk-important by the panel based on their experience.
  - Whether the HBSCs selected would be of benefit to the closure of other GDA issues.

225. The application of the above criteria identified the following sample of HBSCs which formed the basis for my assessment:

- Type A: HEPE-PCS-XVM-CL-V023 Passive Containment Coolant System (PCS) manual valve PCS-PL-V203 unintentionally left closed.
- Type C: HEP-ADS4-C1 Operator fails to depressurize the Reactor Coolant System (RCS) with Automatic Depressurisation System (ADS) Stage 4 on low Core Make-up Tank (CMT) level.
- Type C: HEPO-COG-CONT Operator fails to diagnose high containment pressure
- Type C: HEPO-COGCORECOOLING Operator fails to diagnose inadequate core cooling
- Type C: HEPO-FI-ADSDIS Operator fails to open breakers to prevent spurious ADS Stage 4 actuation

- Type C: HEPO-FI-MCREVAC Main control room evacuation due to fire
- Type C: HEPO-INJ Operator fails to actuate IRWST injection
- Type C: HEPO-L2-CAVFLD Operator fails to flood RV cavity for IVR on loss of core cooling cue
- Type C: HEPO-L2-CNT Operator fails to manually isolate containment
- Type C: HEPO-L2-H2I Operator fails to manually actuate hydrogen ignitors
- Type C: HEPO-OFILL Operator fails to isolate ruptured SG (on High-3 NR SG level—PMS backup)
- Type C: HEPO-PRHR-GT Operator fails to actuate Passive Residual Heat Removal (PRHR) during an event without a Safeguards signal
- Type C: HEPO-RNSINJ Operator fails to align RNS for injection
- Type C: HEPO-RRWSTISO Operator fails to isolate IRWST recirculation following spurious recirculation actuation
- Type A: OPR-011 Maintenance error leads to failure of ADS Stage 4 and IRWST gravity injection squib valves
- Type B: OPR-099 Operator incorrectly executes the CMT discharge valves operability test
- Type A: OPR-106 Maintenance error leads to failure of recirculation squib valves
- Type B: OPR-131 Operator improperly seats the fuel assembly within the core
- BDB-005: Operators provide makeup to the PCCWST and SFP from the PCCAWST with the offsite pump
- BDB-006: Operators provide makeup to the SFP by gravity drain from the PCCWST

Annex 2: SAPs Considered As Part of My Assessment

SAP No	SAP Title	Description
EHF.1	Integration within design, assessment and management	A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility's lifecycle.
EHF.2	Allocation of safety actions	When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.
EHF.3	Identification of actions impacting safety	A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.
EHF.4	Identification of administrative controls	Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.
EHF.5	Task analysis	Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute.
EHF.6	Workspace design	Workspaces in which operations (including maintenance activities) are conducted should be designed to support reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors.
EHF.7	User interfaces	Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.
EHF.8	Personnel competence	A systematic approach to the identification and delivery of personnel competence should be applied.
EHF.9	Procedures	Procedures should be produced to support reliable human performance during activities that could impact on safety.
EHF.10	Human reliability	Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.
EHF.11	Staffing levels	There should be sufficient competent personnel available to operate the facility in all operational states.
EHF.12	Fitness for duty	A management process should be in place to ensure the fitness for duty of personnel to perform all safety actions identified in the safety case.
SC.4	The regulatory assessment of safety cases, safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
EKP.3	Defence in depth	Nuclear facilities should be designed and operated so that defence in depth against potentially

SAP No	SAP Title	Description
		significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	Safety measures	Safety measures should be identified to deliver the required safety function(s).
ERL.3	Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.
ESS.5	Plant interfaces	The interfaces between the safety system and the plant to detect a fault condition and bring about a stable, safe state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour.
ESS.8	Automatic initiation	For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).
ESS.9	Time for human intervention	Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient.
ESS.13	Confirmation to operating personnel	There should be direct means of confirming to operating personnel: (a) that a demand for safety system action has arisen; (b) that the safety systems have operated (actuated) fully and correctly; and (c) whether any limiting condition (operating rule) has been exceeded which takes the safety system beyond its substantiated capability (see Principle ESS.10).
ESS.14	Self-resetting of safety systems	Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent status of the initiating fault.
ESS.15	Alteration of configuration, operational logic or associated data	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) can be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.
ESS.18	Failure independence	No design basis event should disable a safety system.
ESR.1	Provision in control rooms and other locations	Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.
ESR.3	Provision of controls	Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules).
ESR.7	Communications systems	Adequate communications systems should be provided to enable information and instructions to be

SAP No	SAP Title	Description
		transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.
FA.1	Design basis analysis, PSA and severe accident analysis	Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP.
FA.2	Identification of initiating faults	Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.
FA.5	Initiating faults	The safety case should list all initiating faults that are included within the design basis analysis of the facility.
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety. Where safety functions are delivered or supported by human action, these human actions should be identified and classified on the basis of those functions and their significance to safety (see Principle EHF. 3). The methods used for determining the classification should be analogous to those used for classifying structures, systems and components.
ECS.5	Use of experience, tests or analysis	In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the structure, system or component will perform its safety function(s) to a level commensurate with its classification.

Annex 3: List of HBSCs Contained within Westinghouse submissions

UKP-GW-GL-069, Rev. 0, “Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 PRA Update” 7 HBSCs analysed.

- ATW-MAN11: Operator failure to recognize need for manual boration.
- CVN-MAN02: Operator failure to manually align CVCS in boration mode.
- HPM-MAN01: Operator failure to diagnose need for HPHR.
- PRI-MAN01: Operator failure to isolate failed PRHR heat exchanger.
- PRN-MAN01: Operator failure to align PRHR system – loss of MFW.
- PRN-MAN02: Operator failure to align PRHR system – LOCA.
- PRN-MAN03: Operator failure to stop/restart PRHR given a main steam line break.

UKP-GW-GL-070, Rev. 0, UK AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PRA.

- OPA-1: Failure to De-energize the Protection and Safety Monitoring System (PMS) Division Involved in a Fire.
- OPA-2: Operator fails to open manual valve to sprinklers in containment.
- SGDTM: Security guard fails to diagnose that water is leaking and fails to mitigate by opening the annex building front door.
- CRDET: Control room personnel fail to respond to the fire protection system alarms and notify auxiliary personnel to investigate (flood).
- SGCCR: Security guard fails to call control room personnel.
- FLISM: Auxiliary personnel fail to isolate or mitigate the flood.

UKP-GW-GL-071,Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 Low Power and Shutdown PRA.

- LPM-MAN05: Operator fails to recognise the need for RCS Depressurisation.
- REN-MAN02: Operator fails to initiate recirculation during LOCA.
- RHN-MAN05: Operator fails to initiate gravity injection from IRWST via RNS suction line.
- RHN-MAN02: Operator fails to align normal heat removal system.
- RHN-MAN04: Operator fails to isolate the RNS during shutdown conditions.
- ZON-MAN01: Operator fails to start the onsite standby diesel generators during loss of offsite power.
- OPR-093: Maintenance error leads to inability to open RNS Isolation Valves.
- OPR-149: Improper RNS Valve Alignment when Restoring SFS cooling.
- OPR-158: Calibration error allows CVS let-down to lower level below mid-loop resulting in a loss of RNS.

UKP-GW-GL-072 Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Potential Improvements As Proposed in the ALARP Analysis.

UKP-GW-GL-073, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Identified Non-Core Damage Human Errors with Possible Radioactive Release.

- OPR-115: Maintenance leads to Passive Containment Cooling System (PCS) motor-operated outlet valves left closed.
- OPR-116: Maintenance leads to PCS air operated valves fail to open when demanded.
- OPR-118: Failure to maintain PCS storage tank within required temperature band.
- OPR-121: Operator fails to maintain PCS storage tank above minimum level.
- OPR-122: Maintenance error leads to inability to monitor PCS storage tank level.
- OPR-123: Calibration error leads to PCS failing to actuate on high containment pressure via PMS.

UKP-GW-GL-074, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability.

UKP-GW-GL-075, Rev. 0, Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults.

- OPR-204: Operator places fuel assembly in wrong core location.
- OPR-209: Polar crane operator violates safe load path and inadvertently drops a heavy load onto the top of the core resulting in fuel damage.
- OPR-210: Incorrect maintenance performed on the polar crane hoist interlock.
- OPR-104: Operator improperly aligns WGS vent and drain valves during valve line ups.
- OPR-105: Mis-calibration of plant stack radiation monitor.
- OPR-108: Incorrect alignment of Liquid Waste System (WLS) vent and drain valves.
- OPR-110: Mis-operation of the Liquid Rad-waste discharge valve V223.
- OPR-111: Mis-calibration of Liquid Rad-waste Discharge Radiation Monitor (RE229).
- OPR-193: Failure to recognize high tank level (Liquid Waste) and stop transfer pump operation can cause tank to fail.

UKP-GW-GL-076, Rev. 0, “Supplemental Information for the UK AP1000 Human Factors Safety Case – Operator Error Mechanisms”.

- OPR-010: Operator incorrectly executes the CMT discharge valves operability test. An example of a task performed from the main control room (MCR), though sometimes with local plant operator assistance..
- OPR-011: Maintenance error leads to failure of ADS Stage 4 and IRWST gravity injection squib valves. An example of an on-plant service and repair task
- OPR-099: Operator incorrectly executes the CMT discharge valves operability test (bounded by OPR-10).
- OPR-106: Bounded by OPR-11.
- OPR-130: Improper latching of a fuel assembly.
- OPR-131: The operator improperly seats the fuel assembly within the core
- ADN-MAN01: Operator fails to manually actuate the ADS.

- LPM-MAN02: Bounded by AND-MAN-01
- CIB-MAN-00: Bounded by CIB-MAN01. Failure to close the main steam isolation valve on a ruptured steam generator.
- RHN-MAN02: Operator fails to isolate the RNS during shutdown conditions.
- OPA-01: Operator fails to deactivate the PMS division involved in a fire.

[redacted]

[redacted]

[redacted]

Annex 5: List of Step 4 Assessment Findings Which Have Informed My Assessment

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- AF-AP1000-HF-19 The licensee shall model cognitive activation behaviour in the HRA revision.
- 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.
- 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.
- AF-AP1000-HF-22 The licensee shall justify the stress modifiers applied to recovery situations as part of the update to the HRA.
- AF-AP1000-HF-23 The licensee shall provide additional qualitative evidence relating to dependency factors associated with human failure event LPM-REC01.
- 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.
- AF-AP1000-HF-25 The licensee shall provide additional qualitative evidence relating to dependency factors associated with HFEs ADF-MAN01 and CVN-MAN0.
- AF-AP1000-HF-26 The licensee shall reassess the dependency level assigned to HFE PCNMAN01 as part of the HRA update.
- AF-AP1000-HF-27 The licensee shall reassess the modelling associated with HFE CIBMAN01 as part of the HRA update.
- 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.

- AF-AP1000-HF-30 The licensee shall specifically include maintenance and maintainability issues in their Human Factors V&V programme.
- AF-AP1000-HF-33 The licensee shall undertake, or justify otherwise, additional task analysis relating to non ‘core’ areas on a proportionate basis.
- 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.
- AF-AP1000-HF-41 The licensee shall justify or redevelop the scope of the Westinghouse proposals for V&V and ISV
- AF-AP1000-HF-43 The licensee shall provide estimates of maintenance times linked to the PSA system unavailability goals.
- AF-AP1000-HF-46 The licensee shall review and provide further analysis relating to the scenarios of the Westinghouse Operational Sequence Analysis 1.
- AF-AP1000-HF-49 The licensee shall review, reconsider and supplement the task analyses for MTIS tasks on a proportionate and targeted basis.
- AF-AP1000-HF-53 The licensee shall review maintenance access dimensions; recognising the likely equipment (access) requirements.
- 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.

Annex 6: Screenshots of Phase 2 HEA pro-forma – UKP-GW-GL-126

<table>
<tr><th colspan="13">Action Description</th></tr>
<tr><td>Action UIN</td><td colspan="5">This provides the human action's unique identifying number to identify the action.</td><td>Action Error Type</td><td colspan="6">This is where the IAEA Error type (Type A, B, or C) is listed for the action.</td></tr>
<tr><td>Action Title</td><td colspan="12">This is a one sentence description of the successful completion of the action.</td></tr>
<tr><td>Action Context</td><td colspan="12">This is section provides a description of the context in which the action is taken, additional information may describe when this action is performed and if the scenario is shared among other action assessments.</td></tr>
<tr><td>Scenario Description</td><td colspan="12">This describes the scenario in which the action occurs, what has happened up to the point where the action is necessary, and a description of the required action. This section also provides a place for additional information about the action, such as the inclusion of the action in the standard AP1000 plant integrated systems validation test and findings.</td></tr>
<tr><td rowspan="3">Which Mode of Operation was the plant in at the start of the scenario?</td><td colspan="2">Mode 1
At Power</td><td colspan="2">Mode 2
Start-up</td><td colspan="2">Mode 3
Hot Standby</td><td colspan="2">Mode 4
Safe Shutdown</td><td colspan="2">Mode 5
Cold Shutdown</td><td>Mode 6
Refuelling</td></tr>
<tr><td colspan="2">☐</td><td colspan="2">☐</td><td colspan="2">☐</td><td colspan="2">☐</td><td colspan="2">☐</td><td>☐</td></tr>
<tr><td colspan="12">The boxes above indicate the mode of operation of the plant at the beginning of the scenario in which the action occurs. These modes are based on the technical specification (Reference [58]) of the modes based on the reactivity condition, percent rated thermal power, reactor vessel head closure bolts, and the average reactor coolant temperature.</td></tr>
<tr><td>What is the plant state or transient condition when the operator action is conducted?</td><td colspan="12">This describes in more detail the conditions of the plant at the time when the action takes place.</td></tr>
<tr><td rowspan="3">Any special circumstances or hazards to which the Operator Action relates?</td><td>Fire</td><td>Flood</td><td>RA Release</td><td>Pressure Failure</td><td>Explosion</td><td>Toxic, Corrosive</td><td>Dropped Loads</td><td>Seismic</td><td>Severe Accident</td><td>Post-Core Damage</td><td>Post-72 hr BDB</td></tr>
<tr><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td colspan="12">The boxes above indicate any special conditions that may be occurring during this scenario and are therefore relevant to the context in which the action occurs.</td></tr>
</table>

Cues, Alarms, Indications, and System Feedback	
What is the primary Cue, Alarm or Indication to initiate the Operator action?	*This section describes the primary alarm or cue which indicates to the operators that this action should be performed.*
Are there any secondary Cues or Indications to inform need for action?	*This section describes the secondary alarms or cues that also indicate that the action should be performed but generally occur after the primary cue. These can include but are not limited to: indications, other alarms, procedure steps or prompts from the computerised procedure system (CPS), communications from other operators, sounds, etc.*
What are the system feedback mechanisms to confirm process initiation and/or progress?	*This section describes the feedback the system provides to confirm the action has been initiated or is progressing as indicated by items such as but not limited to: indications, alarms, and even (where applicable) sounds or sensations (such as hearing a clank/feeling something physically latch, etc.).*
What are the success criteria and system feedback indications for the task/action?	*This section describes the criteria required for successful completion of the action and the feedback the operators will receive from the system to confirm the completion.*
Timeline/Task Analysis	
Timeline/Task Analysis	*This section is for providing a detailed description of the timing or sequence of steps required to successfully complete the action. Due to the size of these tables, they have been moved to a different section to provide better viewing (see Table 4-3). Some actions were partially or fully bounded by the ISV trials, in which case this section contains those results instead of or in addition to a timeline and task analysis.*
Error Analysis	
Failure Path Analysis	*This section includes the failure path diagram, if it is small enough to be easily read while inside this table field. If the diagram is too large to be legible, it is moved to a separate section following the Timeline/Task Analysis Table. See Section A.16.5 for an example of a separate failure path diagram.* *In some cases (e.g., some Type A maintenance actions), a failure path analysis may not provide the desired insight into the action. In this case, or in addition to the failure path diagram, this section may include discussion of the consequences of failure of particular steps of the action.*

Error Mechanisms	*This section provides a compilation of the error mechanisms that were identified in the action assessment and the Timeline/Task Analysis table. Using the framework of NUREG-2114, as discussed in Section 3.2, the most plausible failure mechanisms were selected and mentioned here. Special care was taken to consider the potential for operators to misdiagnose (misunderstand) what is happening both in the most formal sense (e.g., "this is a LOCA event") and in a more general sense (e.g., understanding what they are doing and why). This section summarises what the error mechanisms are for the operators and if they are likely or unlikely. If needed, an explanation is provided of why the error mechanism is expected to occur or not occur.*	
Performance Shaping Factors	**Key Performance Shaping Factors**	**Description of Claimed Positive or Negative Impact on Task Success**
PSF	*This contains a list of the key performance shaping factors that will drive performance of this action, either in a positive or negative manner. See Section 3.2 for the list of PSFs used in the assessments. Additional PSFs based on NUREG-2114 may be identified as applicable.*	*This section describes in detail the PSF's impact on the task success.* *Rows are added as needed.*
Failure Consequence(s)	*This section describes the consequences of failing this action.*	
Recovery Opportunity(ies)	*This section identifies opportunities for recovery of failure of the action (e.g., peer/supervisor check, post-maintenance operability test, alarm, procedural instruction (e.g., from the continuous action page or the CSFT), etc.*	
Workload	*This section assesses the workload of the operators, taking into consideration the particular circumstances of the actions and parallel work.*	
Procedure	*This section identifies the procedure's ability to get the crew through the completion of the action (within the available time window). The procedures were looked at to identify any do-loops or garden paths that may consume time or send the crew down the wrong path. Additionally the format and design of the procedure, the readability and understandability, any double-negatives, other relevant guiding procedures, such as Conduct of Operations, any background materials, maintenance philosophy documents etc. were also considered.*	
Action Environment		
Any sub-optimal environmental conditions at the operator's location?	*This section identifies any sub-optimal environmental conditions such as; space constraints, radiation shine/shielding, noise, work at height, fire alarms, etc.*	
Any special MTIS tools or PPE required?	*This section identifies any special maintenance test and inspection (MTIS) tools or personal protective equipment (PPE) required to perform the action.*	

Assessment Summary	
Key Performance Driver(s) and Assessment Conclusion(s)	*This section provides an overview of the key performance drivers and what effect they are expected to have on the completion of the action. This section will also discuss what the likely challenges are to be and how they may impact the likelihood of success or failure. There will also be an assessment of how likely it is that the action will be successful, based on the task analysis, opportunities for recovery/restoration, and identification of performance drivers.*
Assumptions Register	
Procedures (PROC)	*These sections record all of the assumptions made in this action assessment, based on the Assumptions Register.*
Staffing (STAFF)	
Training (TRAIN)	
Fitness for Duty (FIT)	
Operation Management and Leadership (MGMT)	
Human Performance Tools and Implementation (HuP)	
Nuclear Safety Culture (SAFE)	
Human-System Interface (HSI)	
Other	
Additional Information/Related Actions	
	This section is used for any additional information or identifying any action(s) that are related to the current action. Rows are added as necessary.

Task #	Event/Plant Response	Operator Task/Response	Est. Time	Cum. Time	Error Types/ Mechanisms	Relevant PSFs	Assumptions	Notes
The step order number or procedure step number.	*This field describes the **AP1000** plant response during the particular step.* *Rows are added as needed.*	*This is generally a direct copy of the procedure step(s), although it may be modified for clarity.*	*Estimated time for the step (see Section 4.1.2). If multiple responses are required for a single procedural step then an equation may be placed here to detail how the time was determined.* *Note that timing may not be applicable for certain Type A or Type B actions.*	*Total elapsed time since t = 0.*	*This section lists and describes the most likely error types or error mechanisms that could occur on this subtask.* *At a minimum this section will be filled out for the critical subtasks, but may additionally be filled out for any subtasks that are part of the action being assessed.*	*This field identifies the relevant PSFs for the subtask, and may also make a statement about the judged effect of the PSF.* *At a minimum this section will be filled out for the critical subtasks, but may additionally be filled out for any subtasks that are part of the action being assessed*	*This field identifies the particular assumptions that relevant to the subtask, based on the Assumptions Register.* *At a minimum this section will be filled out for the critical subtask, but may additionally be filled out for any subtasks that are part of the action being assessed*	*This field provides any additional information relevant to or that provides clarity on the subtask.*