

Generic Design Assessment – New Civil Reactor Build
Step 4 Mechanical Engineering Assessment of the Westinghouse AP1000[®] Reactor

Assessment Report: ONR-GDA-AR-11-010
Revision 0
11 November 2011

COPYRIGHT

© Crown copyright 2011

First published December 2011

You may reuse this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view the licence visit www.nationalarchives.gov.uk/doc/open-government-licence/, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email psi@nationalarchives.gsi.gov.uk.

Some images and illustrations may not be owned by the Crown so cannot be reproduced without permission of the copyright owner. Enquiries should be sent to copyright@hse.gsi.gov.uk.

Unless otherwise stated, all corporate names, logos, and Registered® and Trademark™ products mentioned in this Web site belong to one or more of the respective Companies or their respective licensors. They may not be used or reproduced in any manner without the prior written agreement of the owner(s).

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

PREFACE

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

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000[®] reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires Westinghouse to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the Westinghouse AP1000[®] reactor.

EXECUTIVE SUMMARY

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

This assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 3 the claims made by Westinghouse were examined, followed by the arguments that underpin those claims.

The scope of the Step 4 assessment was to review the safety aspects of the AP1000 reactor in greater detail, by examining the evidence, supporting arguments and claims made in the safety documentation, building on the assessments already carried out for Step 3, and to make a judgement on the adequacy of the Mechanical Engineering information contained within the PCSR and supporting documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific, or generic weaknesses, in the safety case. To identify the sampling for the Mechanical Engineering an assessment plan for Step 4 was set-out in advance.

This assessment has focussed on the safety functions of reactivity control, heat transfer and removal, and containment of radioactive substances, associated with mechanical equipment and systems. In this sense it represents a 'bottom up' assessment, and I have endeavoured to encompass the full range of mechanical items and systems important to safety, albeit subject to the limitations of sampling, to ensure that there are no significant weaknesses in the AP1000 Mechanical Engineering design.

For the UK generic design much of the submission has been restricted to the level of high level specifications which has limited the extent of my assessment. This restriction specifically applies to information from Factory Acceptance Tests and Site Acceptance Tests, which in general form an important suite of evidential information from a Mechanical Engineering assessment perspective. I recognise that this information is not available within GDA since in many cases suppliers have not yet been selected, and in any case, much of this information is not appropriate for such a generic assessment. However, in order to gain confidence in the Mechanical Engineering design, I have assessed the process described by Westinghouse in this respect, discussed examples of such information from other projects, and drawn conclusions accordingly.

I have assessed a broad range of equipment types with important safety functions, including cranes used for nuclear lifting, nuclear ventilation systems, pumps and valves, heat exchangers and associated heat transport systems, Control Rod Drive Mechanisms, and mechanical handling systems. In particular, through undertaking my Step 4 assessment, I have sought to confirm that the equipment described has an adequate nuclear engineering pedigree, is supported by an appropriate degree of Operational Experience Feedback, and has an adequate nuclear safety classification. Where I have identified equipment or processes which I consider to be novel, or which are not aligned to my initial expectations, then I have undertaken a more detailed 'deep slice' assessment. My assessment of the squib valve designs used as part of the Passive Core Cooling System is an example of such a 'deep slice' assessment.

I have also taken a particular interest in the safety classification of mechanical equipment. This is part of the graded approach to safety, to ensure that design, procurement, operational, and maintenance attention is focussed proportionately on equipment with higher safety importance. In particular, and through Step 4 interactions, Westinghouse has now recognised the need to classify duty systems with important safety functions at an appropriate level. These duty systems are the

parts of the Nuclear Power Plant which operate under normal conditions, but whose failure is the initiating event for a fault sequence.

Westinghouse has also agreed to make some important changes to the nuclear ventilation system as a result of interactions within GDA. This includes raising the height of the nuclear ventilation discharge stack to a level above the adjacent containment building, in line with UK expectations, and also the provision of passive High Efficiency Particulate Arrestor (HEPA) filtration to additional areas of the plant.

In some areas where there has been a lack of detailed information Nuclear Directorate (ND) will need additional information in Phase 2 (Site Licensing) and these requirements are identified as Assessment Findings to be carried forward as normal regulatory business. These are listed in Annex 1.

An example of an Assessment Finding is that the AP1000 diesel engines and systems do not adequately take into account the regulation amendment in respect of fuels, Motor Fuel (Composition and Content) Regulations 1999. The AP1000 uses diesel engines to provide stand-by power supply capability to the Nuclear Power Plant electrical load requirements, which is a standard feature of Nuclear Power Plants throughout the world. However, the reliability of the engines starting and continuing to operate on demand can be adversely affected by changes in fuel composition, and this needs to be adequately accounted for in the diesel design and maintenance arrangements.

Some of the observations identified within this report are of particular significance and will require resolution before HSE would agree to the commencement of nuclear safety related construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary these relate to:

- Engineering substantiation for the Mechanical Engineering (including pyrotechnic aspects) of the squib valve designs. The squib valves are fast acting valves used as part of the Passive Core Cooling System within the AP1000, and are novel designs which have been under development during GDA. Although the design development and associated prototype testing have made some good progress, due to the importance of these valves, the lack of finalised substantiation documentation, and associated justification shortfalls, I am not yet satisfied from a Mechanical Engineering perspective.
- Metrication of mechanical equipment to meet UK expectations. It is the UK Regulator's expectation that an AP1000 built in the UK will be a metric design. Although the AP1000 was originally conceived in imperial units, significant progress has been made in this area to meet the UK expectations. However, further work is still required, and a number of exceptions proposed by Westinghouse are either not acceptable, or require further definition and justification.
- Provision of adequate design features to enable the safe isolation and drainage of pipework for Examination, Maintenance, Inspection and Testing (EMIT) activities. Space is limited within the AP1000 design, and there are limited features to enable the safe isolation and drainage of pipework. Westinghouse has also proposed the use of pipe freezing as a routine activity. Further design work and justification is required in this area.

Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic AP1000 reactor design. The AP1000 reactor is therefore suitable for construction in the UK, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes

available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

FOREWORD

Mechanical Engineering

In carrying out this assessment, the term 'Mechanical Engineering' encompasses structures, systems and components (SSCs) that generally contain dynamic elements and interfaces. This is to distinguish it from the discipline of Structural Integrity, which is concerned with SSCs which are static in nature, primarily focussing on containment safety function pressure boundaries. Notwithstanding this definition, a number of static components will also be of interest to the Mechanical Engineering discipline, and subject to appropriate assessment.

Examples of dynamic SSCs that are considered to be of interest include:

- Control Rod Drive Mechanisms.
- Pumps.
- Valves, (check valves, motor operated valves, safety relief valves, squib valves, and isolation valves).
- Cranes.
- Mechanical handling systems.
- Nuclear ventilation systems used to augment nuclear containment barriers.
- Heating Ventilation and Air Conditioning (HVAC).
- Diesel generators.

Examples of static SSCs that are considered to be of interest include:

- Heat exchangers.
- Gloveboxes, cabinets.
- Stillages.
- Seals.
- Strainers.

Structural Integrity aspects with reference to the containment safety function pressure boundaries and vessel internals are not specifically considered or assessed under the Mechanical Engineering discipline. These aspects are the subject of assessment under the discipline of Structural Integrity and reported in the assessment report covering that topic.

LIST OF ABBREVIATIONS

AC	Alternating Current
ACOP	Approved Code of Practice
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
AOV	Air Operated Valve
ASME	American Society of Mechanical Engineers
BMS	Business Management System
ASN	Autorité de Sûreté Nucléaire (French nuclear safety authority)
BOP	Balance Of Plant
C&I	Control and Instrumentation
CAP	Corrective Action Process
CCS	Component Cooling Water System
CFC	Certified For Construction
CMT	Core Make-up Tank
CNSC	Canada Nuclear Safety Commission
COMIT	Constructability, Operability, Maintainability, Testability
CRDM	Control Rod Drive Mechanisms
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DBA	Design Basis Analysis
DC	Direct Current
DCP	Design Change Proposal
DNB	Departure from Nucleate Boiling
DOE	US Department of Energy
DP	Differential Pressure
E&DCR	Engineering and Design Coordination Report
EDCD	European Design Control Document
EIC	Electronic Ignition Circuit
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection and Testing
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
FA	Fuel Assembly
FAT	Factory Acceptance Tests
FDR	Final Design Review

LIST OF ABBREVIATIONS

FHM	Fuel Handling Machine
FMEA	Failure Modes and Effects Analysis
FOAK	First of A Kind
FWS	Feed Water System
GDA	Generic Design Assessment
GE	General Electric
GPM	US gallons per minute
HEPA	High Efficiency Particulate Arrestor
HSE	Health and Safety Executive
HVAC	Heating Ventilation and Air Conditioning
HP	High Pressure
IAEA	International Atomic Energy Agency
IRWST	In-containment Re-fuelling Water Storage Tank
INPO	Institute of Nuclear Power Operators
IRS	Incident Reporting System
LC	Licence Condition
LOCA	Loss of Coolant Accident
LOLER	Lifting Operations and Lifting Equipment Regulations
LP	Low Pressure
LTOP	Low Temperature Overpressure Protection
LTOPS	Low Temperature Overpressure Protection System
MCR	Main Control Room
MDEP	Multi Discipline Evaluation Programme
MOV	Motor Operated Valve
MPPS	Most Penetrating Particle Size
MSLB	Main Steam Line Break
MSQA	Management of Safety and Quality Assurance
MSSV	Main Steam Safety Valve
MTBF	Mean Time between Failure
NASA	(United States) National Aeronautics and Space Administration
ND	Nuclear Directorate
NEA	Nuclear Energy Agency (of the OECD)
NPP	Nuclear Power Plant
NPSH	Net Positive Suction Head
NSC	China Nuclear Safety Centre
NSSS	Nuclear Steam Supply System

LIST OF ABBREVIATIONS

OECD	Organisation for Economic Co-operation and Development
OEF	Operational Experience Feedback
ONR	Office for Nuclear Regulation
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PFD	Probability of Failure on Demand
PHE	Plate (and frame) Heat Exchangers
PLC	Programmable Logic Controller
PMS	Protection and Safety Monitoring System
PORV	Power Operated Relief Valve
PRHR HX	Passive Residual Heat Removal Heat Exchanger
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
PUWER	Provision and Use of Work Equipment Regulations
PXS	Passive Core Cooling System
QA	Quality Assurance
RCCA	Rod Cluster Control Assembly
RCDT	Reactor Coolant Drain Tank
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
RPV	Reactor Pressure Vessel
SAD	Safety and Arming Device
SAP	Safety Assessment Principle
SAT	Site Acceptance Test
SFP	Spent Fuel Pool
SFS	Spent Fuel Pool Cooling System
SQEP	Suitably Qualified and Experienced Person
SSC	Structures, Systems and Components
SWS	Service Water System
TAG	Technical Assessment Guide
TQ	Technical Query
UK	United Kingdom

LIST OF ABBREVIATIONS

US	United States (of America)
US NRC	United States Nuclear Regulatory Commission
VAS	Radiologically Controlled Area Ventilation System
VBS	Nuclear Island Nonradioactive Ventilation System
VCS	Containment Recirculation Cooling System
VES	Main Control Room Emergency Ventilation System
VFS	Containment Air Filtration System
VHS	Ventilation (Hot Machine Shop)
VRS	Radwaste Building Ventilation System
VTB	Turbine Building Ventilation System
WENRA	Western European Nuclear Regulators' Association
WLS	Liquid Radwaste System
WRS	Radioactive Waste Drain System
WSS	Solid Radwaste System
WWS	Waste Water System
ZOI	Zone Of Influence

TABLE OF CONTENTS

1	INTRODUCTION.....	1
2	NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR MECHANICAL ENGINEERING	2
2.1	Initial Assessment Plan for Step 4	2
2.2	Standards and Criteria	10
2.3	Assessment Scope	11
2.3.1	Findings from GDA Step 3.....	11
2.3.2	Additional Areas for Step 4 Mechanical Engineering Assessment	12
2.3.3	Use of Technical Support Contractors.....	13
2.3.4	Cross-cutting Topics.....	13
2.3.5	Integration with Other Assessment Topics	13
2.3.6	Out of Scope Items	14
3	WESTINGHOUSE'S SAFETY CASE.....	15
4	GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR MECHANICAL ENGINEERING	16
4.1	Design Process.....	16
4.1.1	Assessment	16
4.1.2	Findings	18
4.2	Safety Function Categorisation and Equipment Classification	19
4.2.1	Assessment	19
4.2.2	Findings	20
4.3	Good Engineering Practice	21
4.3.1	Assessment	21
4.3.2	Findings	26
4.4	Metrication	27
4.4.1	Assessment	27
4.4.2	Findings	31
4.5	Limits and Conditions and EMIT Identification.....	32
4.5.1	Assessment	33
4.5.2	Findings	34
4.6	Codes and Standards	34
4.6.1	Assessment	35
4.6.2	Findings	36
4.7	Control Rod Drive Mechanisms	36
4.7.1	Assessment	37
4.7.2	Findings	44
4.8	Isolation Valves Providing Containment Safety Function	44
4.8.1	Assessment	44
4.8.2	Findings	48
4.9	Check Valves	49
4.9.1	Assessment	49

4.9.2	Findings	56
4.10	Squib Valves	56
4.10.1	Squib Valve Overview.....	57
4.10.2	Assessment	57
4.10.3	Findings	94
4.11	Safety Relief Valves.....	95
4.11.1	Assessment	95
4.11.2	Findings	100
4.12	Reactor Coolant System Pump.....	100
4.12.1	Assessment	101
4.12.2	Findings	107
4.13	Cranes	108
4.13.1	Assessment	108
4.13.2	Findings	112
4.14	Nuclear Ventilation.....	113
4.14.1	Assessment	114
4.14.2	Findings	120
4.15	Gloveboxes and Cabinets.....	121
4.15.1	Assessment	121
4.15.2	Findings	122
4.16	Heat Transfer and Heat Exchangers	122
4.16.1	Assessment	122
4.16.2	Findings	132
4.17	Diesel Generators	133
4.17.1	Assessment	133
4.17.2	Findings	135
4.18	Fuel Handling.....	135
4.18.1	Assessment	135
4.18.2	Findings	137
4.19	Drains and IRWST Sump Screens	137
4.19.1	Assessment	138
4.19.2	Findings	141
4.20	Pond Stillages	141
4.20.1	Assessment	142
4.20.2	Findings	142
4.21	Radiation Waste Containers	142
4.21.1	Assessment	142
4.21.2	Findings	142
4.22	Transportation Flasks	143
4.22.1	Assessment	143
4.22.2	Findings	143
4.23	Containment Doors and Hatches.....	143
4.23.1	Assessment	143
4.23.2	Findings	145

4.24	RPV Leak Detection System.....	145
4.24.1	Assessment	145
4.24.2	Findings	147
4.25	Containment Penetrations and Vacuum Relief	147
4.25.1	Assessment	148
4.25.2	Findings	149
4.26	Steam Generator Feedwater System	149
4.26.1	Assessment	149
4.26.2	Findings	150
4.27	Chemical and Volume Control System	150
4.27.1	Assessment	150
4.27.2	Findings	152
4.28	Overseas Regulatory Interface	152
4.28.1	Bilateral collaboration:	153
4.28.2	Multilateral collaboration:	153
4.29	Interface with Other Regulators	153
4.30	Other Health and Safety Legislation	153
5	CONCLUSIONS	154
5.1	Key Findings from the Step 4 Assessment	154
5.1.1	Assessment Findings.....	154
5.1.2	GDA Issues.....	154

Tables

Table 1:	Relevant Safety Assessment Principles for Mechanical Engineering Considered During Step 4
----------	-------------------------------------------------------------------------------------------

Annexes

Annex 1:	Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business - Mechanical Engineering – AP1000.
Annex 2:	GDA Issues – Mechanical Engineering – AP1000.

Figures

Figure 1	CRDM – Latch Assembly Arrangement.
Figure 2	ADS Stages 1, 2 & 3 – Schematic Flow Diagram.
Figure 3	Passive Safety Injection - Schematic Flow Diagram
Figure 4	AP1000 Automatic Depressurisation System - Schematic Flow Diagram.
Figure 5	Passive Residual Heat Exchanger – Schematic Flow Diagram.

1 INTRODUCTION

- 1 This report presents the findings of the Step 4 Mechanical Engineering assessment of the AP1000 reactor Pre-Construction Safety Report (PCSR) (Ref. 13) and supporting documentation provided by Westinghouse under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. The approach taken was to assess the principal submission, i.e. the PCSR and the supporting evidentiary information derived from the Master Submission List (Ref. 15), and then undertake assessment of the relevant supporting documentation on a sampling basis in accordance with the requirements of Nuclear Directorate's (ND) Business Management System (BMS) procedure AST/001 (Ref. 2). The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.
- 2 During the assessment a number of Technical Queries (TQ), and Regulatory Observations (RO) were issued and the responses made by Westinghouse assessed. Where relevant, detailed design information from specific projects for this reactor type has been assessed to build confidence and assist in forming a view as to whether the design intent proposed within the GDA process can be realised.
- 3 A number of items are considered to be outside the scope of the GDA process and hence have not been included in this assessment. These are described in Section 2.3.6.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR MECHANICAL ENGINEERING

4 The intended assessment strategy for Step 4 for the Mechanical Engineering topic area was set out in an assessment plan (Ref. 1) that identified the intended scope of the assessment and the standards and criteria that would be applied.

2.1 Initial Assessment Plan for Step 4

5 The following table provides a summary of my initial determination of the main elements of the Westinghouse safety case in respect of systems containing mechanical equipment.

Summary of Determination of the Westinghouse Safety Case in Respect of Mechanical Equipment

Primary Safety Function	System	Safety Aspect
Reactivity Control	Control Rod Drive Mechanism (CRDM)	<p>Reactivity control is achieved by the control rods and the soluble boric acid chemical composition within the primary coolant.</p> <p>The CRDMs are of a design that allows a fast response to reactivity changes.</p> <p>Slow changes such as load follow, and fuel burn up is compensated by a combination of mechanical means (gray rods) and boron concentration changes. Typically, the day-to-day fuel burn up and load follow power changes are controlled by the gray rods, and fuel burn reactivity changes are compensated by weekly changes in the boron concentration.</p>
Reactivity Control	Emergency Makeup and Boration	Emergency addition of boric acid provides a diverse method of shutting down the reactor.
Heat transfer / Residual heat removal	Passive Core Cooling System (PXS)	<p>The PXS provides emergency core cooling during events that involve increasing and lowering of secondary side heat removal and the lowering of the reactor coolant system inventory.</p> <p>The system manages reactor core decay heat removal, addition of Boron to the Reactor Coolant System (RCS) and acts as the safety injection system following a Loss of Coolant Accident (LOCA).</p> <p>The passive core cooling system uses four different sources of passive injection during a LOCA. Accumulators provide a very high flow for a limited duration of several minutes if RCS pressure is decreased.</p> <p>The Core Makeup Tanks provide a relatively high flow</p>

Primary Safety Function	System	Safety Aspect
		<p>for a longer duration at any RCS pressure. The In-containment Re-fuelling Water Storage Tank (IRWST) provides a lower flow, but for a much longer time that is driven by gravity head.</p> <p>The Containment is the final long-term source of water, which becomes available following the injection of the other three sources and the flooding of the containment.</p> <p>Pressure Operated Relief Valves protect the tanks from overpressure.</p>
Heat transfer / Residual heat removal	Component Cooling Water System & Service Water System	<p>Provides support to the Normal Residual Heat Removal System (RNS) in cooling down the reactor during the second cool down phase.</p> <p>Removes heat from various components during plant operation and removes core decay heat and other heat during reactor cooling and shutdown.</p>
Heat transfer / Residual heat removal	Chemical & Volume control System (CVS)	<p>Provides borated makeup to the reactor coolant system following accidents such as small loss-of-coolant accidents, steam generator tube rupture events, and small steam line breaks.</p> <p>Isolation of the reactor coolant system upon receipt of a high steam generator level signal or a high pressuriser level signal.</p>
Heat transfer / Residual heat removal	Reactor Coolant System	<p>During normal operations the RCS transfers the heat generated in the reactor to the secondary side loop system.</p> <p>Following a shutdown or a loss of power, the pump flywheel provides the inertia to ensure adequate heat transfer capability and aids the process to establish a natural circulation flow.</p>
Heat transfer / Residual heat removal	Feed Water System (FWS)	<p>The FWS provides an alternative means to the PXS to remove decay heat in a reactor trip scenario. The FWS also provides the means to remove nuclear heat during normal operation.</p>
Containment of radioactive substances	Passive Containment Cooling System	<p>Reduce the containment temperature and pressure following a LOCA or Main Steam Line Break (MSLB) accident.</p> <p>Serves as the means of transferring heat to the ultimate heat sink for other events resulting in a significant increase in containment pressure and temperature.</p> <p>Capable of removing sufficient thermal energy including subsequent decay heat from the containment atmosphere following a design basis event.</p>

Primary Safety Function	System	Safety Aspect
		<p>The passive containment cooling system provides a source of makeup water to the spent fuel pool in the event of a prolonged loss of normal spent fuel pool cooling.</p>
<p>Containment of radioactive substances</p>	<p>Containment Isolation</p>	<p>Upon failure of a main steam line, the steam generators are isolated as required to prevent excessive cool down of the reactor coolant system or over pressurisation of the containment.</p> <p>Provide isolation, containment barrier integrity for fluid and gas systems.</p>
<p>Containment of radioactive substances</p>	<p>Ventilation</p> <p>Annex / Aux Building Non Radioactive Ventilation System</p> <p>Nuclear Island Non Radioactive Ventilation System (VBS)</p> <p>Radiologically Controlled Area Ventilation System (VAS)</p>	<p>Prevents the build-up of hydrogen in Class 2 battery rooms.</p> <p>Provides a contained atmosphere to allow personnel to occupy the control room in the event of a design basis accident. (Positive pressure).</p> <p>Monitors the main control room supply air for radioactive particulate and iodine concentrations</p> <p>Isolates the ventilation penetrations in the main control room boundary on high-high particulate or iodine concentrations in the main control room supply air, or on extended loss of ac power to support operation of the main control room emergency habitability system.</p> <p>Provides a system to manage airborne radioactivity in the access areas at safe levels for plant personnel.</p> <p>Maintains the overall airflow direction within the areas it serves from areas of lower potential airborne contamination to areas of higher potential contamination.</p> <p>Prevents the uncontrolled release of airborne radioactivity to the atmosphere or adjacent clean plant areas.</p> <p>Automatically isolates selected building areas from the outside environment by closing the supply and exhaust duct isolation dampers and starting the containment air</p>

Primary Safety Function	System	Safety Aspect
	<p>Containment Recirculation Cooling System (VCS)</p> <p>Containment Air Filtration System (VFS)</p>	<p>filtration system when high airborne radioactivity in the exhaust air duct or high ambient pressure differential is detected.</p> <p>Provides a containment atmosphere to allow limited access while at power and continuous access while reactor is in a shutdown state, (in conjunction with VFS)</p> <p>Provides an atmosphere to suit safety related equipment, (pumps, CRDMs etc).</p> <p>Reduces the containment temperature, pressure and humidity following a LOCA to manage the release of airborne radioactivity.</p> <p>Controls the containment thermal environment during normal operation.</p> <p>Controls the containment thermal environment for personnel accessibility and equipment operability during refuelling and plant shutdown.</p> <p>Maintains a homogeneous containment temperature and pressure during containment integrated leak rate testing (ILRT).</p> <p>Maintains a homogeneous containment temperature and pressure during a loss of off-site power.</p> <p>Controls the reactor cavity area average concrete temperature.</p> <p>Provides intermittent flow of outdoor air to purge the containment atmosphere of airborne radioactivity during normal plant operation, and continuous flow during hot or cold plant shutdown conditions to provide an acceptable airborne radioactivity level prior to personnel access.</p> <p>Provides intermittent venting of air into and out of the containment to maintain the containment pressure within its desired pressure range during normal plant operation.</p> <p>Directs the exhaust air from the containment atmosphere to the plant vent for monitoring, and provides filtration to limit the release of airborne radioactivity at the site boundary within acceptable levels.</p>

Primary Safety Function	System	Safety Aspect
	Habitability Systems (VBS & VES)	<p>Prevent uncontrolled release of airborne radioactivity to the atmosphere or adjacent clean plant areas.</p> <p>The habitability systems are capable of maintaining the main control room environment suitable for prolonged occupancy throughout the duration of the postulated accidents.</p> <p>A maximum main control room occupancy of up to 11 persons can be accommodated.</p> <p>The emergency habitability system maintains CO2 concentration to less than 0.5 percent for up to 11 main control room occupants.</p> <p>The habitability systems provide the capability to detect and protect main control room personnel from external fire, smoke, and airborne radioactivity.</p> <p>Automatic actuation of the individual systems that perform a habitability systems function is provided. Smoke detectors, radiation detectors, and associated control equipment are installed at various plant locations as necessary to provide the appropriate operation of the systems.</p>
Containment of radioactive substances	Component Cooling Water System	Provide a barrier against leakage of fluid from primary containment and reactor systems.
Containment of radioactive substances	Reactor Coolant System	<p>The RCS acts as the second containment barrier of defence following the fuel cladding.</p> <p>The Reactor Pressure Vessel (RPV) seal arrangement provides a containment barrier.</p> <p>The Safety Relief Valves limit the pressure within the RCS and minimise the possibility of high pressure transient during normal operations and cold over pressurisation transients during cold shut down conditions.</p>

- 6 Based on this determination of mechanical systems and their high level safety functions, and in conjunction with the work already undertaken during Step 3, I then identified the associated mechanical engineering equipment, and processes for assessment as part of my Step 4 activity.
- 7 In particular, through undertaking my Step 4 assessment, I have sought to confirm that the equipment described has an adequate nuclear engineering pedigree, is supported by an appropriate degree of Operational Experience Feedback (OEF), and has an adequate nuclear safety classification. Where I have identified equipment or processes which I

consider to be novel, or which are not aligned to my initial expectations, then I have undertaken a more detailed 'deep slice' assessment. My assessment of the squib valve designs used as part of the Passive Core Cooling System is an example of such a 'deep slice' assessment.

8 My Step 4 plan therefore identified the following initial areas for assessment:

Assessment Area	Description
Design Process: Safety Categorisation and Classification	Assessment of the Safety Categorisation and Classification arrangements, once the methodology is in line with the UK SAPs. Implementation strategy for the revised Safety Categorisation and Classification arrangements within the PCSR, DCDs and the Westinghouse design process.
Design Process: Transfer of Safety Requirements Through the Project Life Cycle	Process for identifying safety functional requirements. Process for transferring the detailed safety functional requirements through the project life cycle. Evidence that the detailed design delivers the required safety functional requirements.
Design Process: Good Engineering Practice	This area will be progressed, including consideration to understanding the Mechanical Engineering items important to safety that will require redesigning, and the items that will have their imperial units transformed, to SI units.
Design Process: Layout / Interfaces	We are interested in further assessment of the RCS pump replacement sequence, once the methodology is at an increased level of definition and understanding; (noting that the design / supplier has recently been changed).
Metrication	Progressing and closing out the RO actions from a Mechanical Engineering perspective.
CRDMs	Safety Categorisation and Classification, once the methodology is in line with the UK Regulatory expectations. Evidence from the CRDM trials. Arguments and evidence that support the CRDM equipment classification.
Design Process: Valve Selection Process	We shall progress assessment in this area following the issue of a number of references.
Isolation Valves (containment safety function)	Safety Categorisation and Classification. Identification of safety functional requirements. Arguments and evidence that support the isolation valve equipment classification. Documentation updates to reflect my assessment findings.
Check Valves	Assessment of the Safety Categorisation and Classification arrangements. Identification of safety functional requirements. Arguments and evidence that support the valve equipment classification.

Assessment Area	Description
Design Process: Safety Categorisation and Classification	Assessment of the Safety Categorisation and Classification arrangements, once the methodology is in line with the UK SAPs. Implementation strategy for the revised Safety Categorisation and Classification arrangements within the PCSR, DCDs and the Westinghouse design process.
Squib Valves	Safety Categorisation and Classification, once the methodology is in line with the UK Regulatory expectations. Progressing and closing out the RO actions. Arguments and evidence that support the squib valve design and equipment classification. Consideration of MDEP findings and recommendations.
Safety Relief Valves	Further evidence in relation to the design and Equipment Qualification issues relating to these Safety Relief Valves, based on their safety classification.
Reactor Coolant System Pump	Safety Categorisation and Classification, once the methodology is in line with the UK Regulatory expectations. Identification of safety functional requirements. Findings and recommendations from the functional testing. Arguments and evidence that support the RCP equipment classification.
Cranes	Further evidence in relation to design issues relating to cranes important to safety, based on their safety classification.
Nuclear Ventilation	Continue the assessment activity in this area, and seek further evidence in relation to the design and Equipment Qualification issues relating to these nuclear ventilation systems, based on their safety classification. Progress Regulatory Observation on the subject of containment and filtration philosophy for areas of the facility subject to potential contamination during normal and fault conditions.
HVAC	Further understanding of the justification of the habitability provision for the Main Control Room under accident conditions.
Gloveboxes / Cabinets	The area will be progressed following a similar approach to the other regulatory areas of interest.
Heat Exchangers	Further assessment activity in this area, with potential attention focussed on evidence to support the Equipment Qualification (EQ) requirements associated with this equipment, based on its safety classification.
Diesel Generator	Supplementary assessment of the diesel generators shall be given consideration, once the allocation of safety categorisation and classification issue is satisfactorily resolved.
Spent Fuel Handling	The area will be progressed following a similar approach to the other regulatory areas of interest specifically: Safety Categorisation and Classification. Identification of safety functional requirements. Incorporation of Operational Experience Feedback.

Assessment Area	Description
Design Process: Safety Categorisation and Classification	Assessment of the Safety Categorisation and Classification arrangements, once the methodology is in line with the UK SAPs. Implementation strategy for the revised Safety Categorisation and Classification arrangements within the PCSR, DCDs and the Westinghouse design process.
Pond Stillages	The area will be considered following a similar approach to the other regulatory areas of interest specifically: Safety Categorisation and Classification. Identification of safety functional requirements. Incorporation of Operational Experience Feedback.
Radiation Waste Containers	The area will be considered following a similar approach to the other regulatory areas of interest specifically: Safety Categorisation and Classification. Identification of safety functional requirements. Incorporation of Operational Experience Feedback.
Transportation Flasks	The area will be considered following a similar approach to the other regulatory areas of interest. specifically: Safety Categorisation and Classification. Identification of safety functional requirements. Incorporation of Operational Experience Feedback.
Component Cooling Water System (CCS)	Identification of components important to safety that have a reliance on the CCS. Safety Categorisation and Classification of the CCS. Identification of safety functional requirements. Arguments and evidence that support the CCS classification.
Mechanical Filters and Strainers	The area will be considered following a similar approach to the other regulatory areas of interest specifically: Safety Categorisation and Classification. Identification of safety functional requirements. Incorporation of Operational Experience Feedback.

2.2 Standards and Criteria

9 The approach has been to carry out this assessment in accordance with :

- ND standards;
- applicable SAPs;
- guidance of the Technical Assessment Guides (TAG).

Those SAPs series considered generally relevant to Mechanical Engineering assessment are listed in Table 1 of this document. Individual SAPs are also detailed within the text of this document against the relevant section.

The Mechanical Engineering assessment has been carried out with the aid of a number of applicable SAPs, which are principles against which regulatory judgements are made and provide fundamental guidance in scoping an assessment topic and in carrying out an effective assessment. This approach ensures the assessment provides a targeted, consistent and transparent consideration on the adequacy of the Westinghouse design.

10 Generally SAPs capture the requirements of Western European Nuclear Regulators' Association (WENRA) reference levels (Ref. 9) and the International Atomic Energy Agency (IAEA) Standards Series requirements.

11 It is worth noting, the nature of the Mechanical Engineering discipline generally drives the assessment down to equipment level. Assessment at this equipment level can be extremely wide ranging given the very large number of such items, with numerous interfaces, across various plant process systems and covering several disciplines. As a consequence, a wide range of SAPS and TAGs can be applicable to carrying out an effective assessment. The approach to carrying out an effective sampled assessment is to select the most appropriate SAPS and TAGs relating to the selected Mechanical Engineering aspect.

2.3 Assessment Scope

12 The Step 4 assessment scope has been primarily developed from the work undertaken during the Step 3 process, and reviewed and expanded as appropriate through liaison with other assessment disciplines, and as derivative lines of enquiry have emerged through progression of the initially identified assessment scope.

2.3.1 Findings from GDA Step 3

13 At the end of Step 3 of the GDA process good progress had been made in terms of reviewing the Westinghouse submission, and identifying issues and areas for more detailed review and discussion. The Step 3 process and findings are described in detail in the report published in November 2009 (Ref. 6).

14 At that stage of the overall GDA process, the following three Regulatory Observations were raised associated with this Westinghouse Submission:

- Regulatory Observation - RO-AP1000-036 - Squib Valve Concept and Design Substantiation, July 2009.
- Regulatory Observation - RO-AP1000-038 – Metrication of the AP1000 for the UK, July 2009.
- Regulatory Observation - RO-AP1000-043 – Nuclear Ventilation, September 2009.

These represent areas that required further justification by, and / or discussion with Westinghouse and further assessment by the Regulators in the expectation that they could be resolved to the satisfaction of the Regulators.

15 The Regulatory Observation in respect of the Squib Valve Concept and Design Substantiation was a particularly significant assessment finding at this time. I had significant concern regarding the state of design and development, and programme for future work, in respect of this Squib Valve concept, used as part of the Passive Core Cooling System and the Reactor Coolant System. I considered that Westinghouse needed to apply significant resource and attention to this area.

16 The Regulatory Observation in respect of Metrication was of interest across a range of assessment disciplines, and represented a cross-cutting matter. However, this observation was particularly important for Mechanical Engineering, with a specific focus on the use of threaded fasteners, and the maintenance implications of using a non metric design.

- 17 The Regulatory Observation in respect of Nuclear Ventilation was raised towards the end of the Step 3 process, and was developed in close consultation with the Environment Agency. I considered that Westinghouse needed to apply significant attention to this area, since nuclear ventilation systems and associated filtration arrangements play a fundamental part in protecting people, society, and the environment from the hazards of radiation.
- 18 The Westinghouse methodology of safety categorisation and classification was not in line with the UK Regulatory expectations. At that stage of the GDA the Westinghouse methodology proved to be an obstacle in carrying out an effective assessment. Westinghouse had started work to align the allocation of safety categorisation and classification to the UK SAPs at the end of Step 3, and I considered this exercise required expediting and completing on an urgent basis otherwise it would significantly impact the effectiveness of the GDA process.
- 19 I also considered the understanding and definition of the installation sequence of the Reactor Coolant System (RCS) pump (chosen as an example due to its size, mass and location) to be at an early stage and I continued to target this aspect during my Step 4 assessment.
- 20 However, a degree of confidence was gained in the design process applied by Westinghouse. Sampled areas that provided this confidence included the:
- RCS pump, which included review of Westinghouse's supply chain and the visible evidence of adequate Quality Assurance.
 - CRDMs and the development tasks that were being undertaken.
 - Valve selection process, where documents assessed captured both operational experience and standardisation aspects.
- However, during the Step 4 assessment process the nominated supplier for the RCS pump changed, and so the assessment activity had to review this new information, and undertake re-work activities as necessary.
- 21 At the end of the Step 3 assessment process, no Regulatory Issues were identified associated with the Westinghouse submission.

2.3.2 Additional Areas for Step 4 Mechanical Engineering Assessment

- 22 The following additional areas for assessment were identified during the Step 4 process, through liaison with other assessment disciplines, or as derivative areas from previously identified lines of enquiry:
- Containment doors and hatches.
 - Reactor Pressure Vessel (RPV) leak detection system.
 - Containment penetrations and vacuum relief.
 - Steam generator feedwater system.
 - Overpressure protection report.
 - Chemical and volume control system.
 - In-containment Re-fuelling Water Storage Tank (IRWST) screens and drainage systems.

2.3.3 Use of Technical Support Contractors

23 No technical support contractors were used to support the Mechanical Engineering assessment of the Westinghouse AP1000 reactor design.

2.3.4 Cross-cutting Topics

24 A number of topics are by their nature 'cross-cutting' (e.g. Probabilistic Safety Analysis (PSA), Management of Safety and Quality Assurance (MSQA)), however in addition to these the project has identified the following 'cross-cutting' sub-topics:

- Severe Accidents.
- Categorisation and Classification.
- Metrication.

I have taken a specific technical interest in the subject of safety function categorisation and equipment classification, both to assist in the overall cross-cutting adoption of a philosophy by Westinghouse which aligns to that described by the UK SAPs, and also since it interfaces directly with Nuclear Site Licence Condition compliance requirements, as described later in this Step 4 report.

I have also taken a lead in the cross-cutting topic of metrication, in terms of providing guidance and clarity in terms of ND expectations across all disciplines. This is described later in this report.

2.3.5 Integration with Other Assessment Topics

25 It is recognised that there are a number of areas where there has been a need to consult with other assessors as part of the assessment process during Step 4. These areas have been overseen by the Project Technical Inspectors in conjunction with Assessment Unit Heads to ensure that potential interactions are captured and that duplicate assessment work is prevented. However, all these dependencies have been 'soft' dependencies such that Mechanical Engineering assessment has progressed and been completed without specific input requirements from these other topics.

26 Coordination with other disciplines has also generally been undertaken as part of the normal assessment process. Given the sampling nature of assessment, this process has proved to be effective and efficient in determining the adequacy of safety cases, and identifying areas of weakness for further resolution.

27 It should be noted that some areas of Mechanical Engineering regulatory interest are electro-mechanical in nature, and specifically the delivery of safety functions may rely on adequate control and instrumentation systems, e.g. nuclear lifting / cranes. Although the general control / protection function of these systems is considered to be a valid area for the Mechanical Engineering assessment discipline initially, where potential regulatory concerns are identified, these are notified to the Control and Instrumentation (C&I) assessment team, who will then take the lead.

2.3.6 Out of Scope Items

28 Westinghouse has stated that no items are out of scope for the GDA Mechanical Engineering assessment. Nevertheless, I consider the following items in reality to be out of scope:

- Final nuclear ventilation stack height confirmation and associated calculations, (final stack characteristics are site dependent).
- Equipment qualification and substantiation reports in general, (documents are strongly linked to the choice of supplier which is outside the GDA scope, although sample information has been provided to illustrate the methodology employed). However, for the squib valves in particular, I have sought more evidence in this area due to the novelty and importance of the designs.
- Furthermore, any Mechanical Engineering features within the AP1000 to support the handling of mixed oxide fuel are outside the scope of GDA. In addition, I have not assessed any features of the design associated with the use and handling of new fuel made from reprocessed uranium.

29 Towards the end of Step 4, and through liaison with the Environment Agency, it became apparent that the description of the Service Water System cooling provision, via two small cooling towers, was different to the information provided in the AP1000 Environment Report (Ref. 67). The Service Water System design described in this Environment Report is a once through cooling system using sea water. My mechanical assessment is based on the closed loop system using cooling towers described by Westinghouse during Step 4, and use of any other cooling system is therefore an out of scope item. Westinghouse has now acknowledged this inconsistency via letter, (Ref. 48), and has stated that the Environment Report has been updated in this area. Further Mechanical Engineering assessment in this area will be undertaken as part of site licensing if required.

3 WESTINGHOUSE'S SAFETY CASE

- 30 A safety case is generally assessed by identifying the claims on structures, systems and components, and people, and then by assessing the associated arguments and underpinning evidence. This assessment structure, which should be aligned to the safety case structure, is essentially a 'top down' approach and provides a logical framework to ensure that all hazards have been adequately identified and suitably addressed.
- 31 The nature of Mechanical Engineering, and associated Mechanical Engineering assessment, favours an alternative 'bottom up' type approach. In this case mechanical items important to safety are identified and then assessed on the basis of their safety function, categorised in functional terms as associated with either reactivity control, heat transfer and removal, or containment of radioactive substances.
- 32 The Westinghouse PCSR (Ref. 13) used as the basis for my assessment does not collate all information relevant to Mechanical Engineering as a separate topic within the document. I have therefore identified references to mechanical equipment from the appropriate safety case chapters, and pursued my assessment accordingly. The equipment and processes I have selected to assess are reported in the following Section 4 of this report. As a result of there being no large Mechanical Engineering submissions to assess, my assessment has been based on a series of meetings with Westinghouse. During these meetings the depth and nature of the Mechanical Engineering design has been tested by questioning, and by the examination of appropriate design information.
- 33 This assessment approach has interfaced with the approach adopted by other disciplines, including coordination with the areas of Fault Studies and Probabilistic Safety Assessment, as well as Internal Hazards, to provide a holistic assessment in terms of claims, arguments and evidence covering Mechanical Engineering items important to safety.

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR MECHANICAL ENGINEERING

4.1 Design Process

34 I have undertaken a sampled assessment of the Westinghouse design process, to ensure they have robust design practices in place that adequately manage interdisciplinary requirements, interfaces, and with the necessary degree of Quality Assurance. I consider this to be an important aspect which underpins the safety justification of the AP1000 design. I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle EQU.1 (Ref. 4) states 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'

35 In undertaking my assessment, I have also used the internal ND technical assessment guide, Design Safety Assurance, T/AST/057 (Ref. 7), to guide my process and conclusions.

4.1.1 Assessment

4.1.1.1 Design Organisation

36 From a GDA perspective I targeted a number of key areas for evidence that I consider important to confirm Westinghouse are an acceptable Responsible Designer, and are able to manage and control a safety important design process. In particular I consider that Westinghouse should have:

- Adequate arrangements in place to transfer the safety functional requirements onto the supplier to allow the detailed design and manufacturing to be carried out. This subject has been generally progressed as part of the lines of enquiry and assessment for the various Mechanical Engineering equipment types. I do not expect this information to be fully complete as part of this generic assessment activity, but consider it to be an Assessment Finding (**AF-AP1000-ME-01**) that all necessary Equipment Qualification requirements are specified as necessary for Phase 2.
- Adequate arrangements in place to enable the identification and subsequent transfer of the plant operating limits and conditions to a future licensee, to allow them to undertake their regulatory duties and to generate adequate plant Operating Rules.
- Adequate arrangements for the identification of items important to safety through an appropriate equipment classification process, to allow adequate design and procurement, and generation of a Plant Maintenance Schedule to support the Examination, Maintenance, Inspection and Testing (EMIT) requirements of Nuclear Site Licence Conditions.

The subject of Operating Rules, safety categorisation and classification, and EMIT is discussed later in Sections 4.2 and 4.5 of this report, as well as under individual equipment topic areas.

37 I consider from a Mechanical Engineering perspective a significant quantity of evidence is only collated from carrying out the Factory Acceptance Tests (FATs – i.e. works tests) and Site Acceptance Tests (SATs - e.g. non-active commissioning tests of equipment, and their integrated system tests). This information is generally not available within GDA, which I consider to be an Assessment Finding (**AF-AP1000-ME-02**). In recognition of this, my Step 4 assessment has focused on the design specifications, processes, and the

transfer of Mechanical Engineering design criteria that are important to safety through to the supply chain, to support the detailed design, procurement and manufacturing phases.

38 However, from my work undertaken during Step 3, and the further work undertaken within Step 4, I am satisfied that Westinghouse do generally have an adequate design process for the specification and control of technical information relating to Mechanical Engineering equipment and systems against SAP EQU.1.

4.1.1.2 Design Change Control

39 I consider that the Responsible Designer should have adequate arrangements to identify, assess, sentence and implement design changes, noting that such changes which are inadequately conceived and / or executed are a recognised threat to nuclear safety.

40 In response to my line of enquiry Westinghouse described the AP1000 Design Change Control tools TQ-AP1000-1262 (Ref. 10). NSNP 3.4.1, Change Control for the AP1000 Program (DCP), covers formal changes to the AP1000 design; APP-GW-GAP-420, Engineering & Departure Change Request, covers procurement / manufacturing / construction inspired changes; APP-GW-GEP-010, Engineering Open Items Procedure, allows work in parallel to progress, perhaps using assumed parameters by one group which subsequently need to be confirmed.

41 In general issue status is denoted by letters, i.e. A, B, C etc for preliminary work, and then as numeric descriptors , i.e. 0, 1, 2, 3 etc for work which has been formally issued.

42 Design Change Proposals (DCPs), are classified as Class 1, 2 or 3, depending on their significance, with class 1 being the most significant. The classification system is as follows:

- Class 1 – licensing basis impact, safety case impact.
- Class 2 – less impact than Class 1, but affects a number of modules, i.e. non local, and with a cost < \$100 000.
- Class 3 – local physical effects only, no impact on other interfacing systems or items, for documentation errors etc, and with a cost < \$25 000.

43 Due to the commencement of physical build in China, and associated cost impact of any changes, all non trivial changes are now typically in class 1 or class 2.

44 All approved changes have to be agreed unanimously, through the due process, and the entire programme follows the same procedure; no DCPs can be closed with an open comment. A formal process is undertaken for Class 1 and Class 2, whereas Class 3 changes are controlled by the normal documentation issue and approval process. DCPs are considered to be archived quality records.

45 The Engineering and Design Coordination Report (E&DCR) process controls locally inspired modifications, which are not automatically imported back into the AP1000 design; it controls design deviations / departures, non-conformances, field change requests and material substitution requests etc.

46 The lowest classification of DCP, Class 3, does not attract a formal DCP number, and Westinghouse stated that the decision to classify at this level effectively rested with the approval manager. I consider that a common regulatory concern is the 'under classifying' of changes, and whilst I recognise that any system needs to be graded, so that attention is focussed appropriately, there is a danger in the Westinghouse system that many

changes are not visible, and there may also be adverse aggregation effects. Westinghouse has stated that visibility is provided through the minutes of regular design review meetings etc, but I am not convinced that this is adequate. In conclusion, I consider it necessary that the future licensee ensures that there is an adequate system for controlling these lower level DCPs; which I consider to be an Assessment Finding (**AF-AP1000-ME-03**).

- 47 I questioned Westinghouse on the process to be followed when a DCP is rejected by the change control board. Westinghouse stated that the change was simply not taken forward, although the reasoning for rejection is captured within their system.
- 48 Within the management system, completion times are designated for various stages of the design change approval process. Documentation impacted by a DCP should be updated within 6 months of formal approval of the DCP, or when six DCPs are impacting the document, or as planned if the document is scheduled for update according to the project programme. However, only Westinghouse documentation is updated through this process, and suppliers' documentation will follow in due course dependant on the status of the applicable contract.
- 49 Engineering and Design Coordination Reports may result in a DCP, if it is decided to reflect the change in the formal AP1000 design for other plants.
- 50 E&DCRs undergo the same discipline review and independent verification as the original affected document. E&DCRs are also archived quality records.
- 51 Westinghouse described the 'open items' process, and stated that their process follows a workflow of 'preliminary', 'design', and then 'CFC' (Certified for Construction) status. It is Westinghouse's intent to issue all CFC documents without any open item, although this is not a requirement, and they may proceed with manufacturing at risk. I consider it to be an Assessment Finding (**AF-AP1000-ME-04**) that a future licensee ensures that the final manufactured items important to safety meet the safety important requirements set forth in the final documentation.
- 52 Notwithstanding these Assessment Findings, I consider this to be a generally well structured and rational process, which I consider to be adequate from a Mechanical Engineering GDA perspective.

4.1.2 Findings

AF-AP1000-ME-01: *The licensee shall generate appropriate evidence that Equipment Qualification is adequately specified for all mechanical items important to safety. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-02: *The licensee shall make available upon request evidence of the detailed design substantiation, FATs information, and SATs information, for individual mechanical items and their associated systems, which are important to safety. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-03: *The licensee shall ensure that design changes associated with the AP1000, specifically including Class 3 DCPs, are adequately controlled, and receive a suitable degree of review and audit, commensurate with their safety*

significance. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

AF-AP1000-ME-04: *The licensee shall ensure that the final manufactured items important to safety meet the safety important requirements set forth in the final design documentation. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.2 Safety Function Categorisation and Equipment Classification

53 Safety function categorisation and associated equipment classification are important considerations from a Mechanical Engineering perspective, although this topic area is cross-cutting in that it affects the range of assessment disciplines to a greater or lesser degree. I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle ECS.1 (Ref. 4) states ‘The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.’
- Safety Assessment Principle ECS.2 (Ref. 4) states ‘Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regards to safety.’

54 It is for Westinghouse to generate their own structure to reflect the principles described above, based on considerations of hazard and risk, but this subject is important for mechanical equipment since it is an input to the definition of design requirements, procurement processes (specifically assurance activities), installation and commissioning activities, and of particular importance the Examination, Maintenance, Inspection and Testing requirements which are regulated during plant operation under Nuclear Site Licence Condition 28.

4.2.1 Assessment

55 During Step 4 Westinghouse described their action plan, which specifically covered their review and re-work associated with meeting the UK regulatory expectations in this cross-cutting area. Westinghouse recognised early in the Step 4 process, and as result of feedback received during Step 3, that their extant system of safety function categorisation and equipment classification was heavily tied to meeting the requirements of the US Regulator, and would not be acceptable in the UK.

56 Westinghouse provided a comparison between the US categorisation / classification system, and that described by the UK SAPs. Their proposals for the AP1000 design categorisation / classification system to meet UK expectations are summarised as follows:

- Category A

Principal means for maintaining nuclear safety; failure has potential for significant core damage or release to the environment within 72 hours of accident, e.g. decay heat removal, reactivity control, MCR habitability, RCS integrity, RCS inventory control, containment heat removal / integrity, spent fuel cooling.

- Category B
Significant contributor to maintaining nuclear safety; failure may reduce safety margins significantly, but not result in a Design Basis Accident, e.g. radwaste system integrity, instruments to monitor category A functions, post 72 hour functions, isolation of control systems which could reduce margins.
- Category C
Contribution to nuclear safety; failure will not result in a Design Basis Accident, e.g. long term support of category A and B functions, beyond Design Basis Accident events, monitoring of environmental releases.

57 For the associated equipment classification levels, Westinghouse described the specified design and quality standards which were applicable, including application of appropriate seismic categories.

58 Some examples covering application of their revised methodology are as follows:

- Passive RHR Heat Exchanger – now Cat A Class 1.
- Start-up feedwater pumps – now Cat A Class 2.
- Standby diesel generators – now Cat A Class 2.

59 Through discussion I provided feedback to Westinghouse that I considered it appropriate that 'duty' system equipment, (referred to as Safety Related Systems within the ND Technical Assessment Guides), are also classified at an appropriate level. These 'duty' systems represent the operational equipment used within a Nuclear Power Plant (NPP), but which have important safety functions (i.e. reactivity control, heat transfer and removal, and containment of radioactive substances), and whose failure is typically the initiating event within a fault sequence. An example of such a 'duty' system is the main containment Polar Crane.

60 At the end of Step 4, I consider Westinghouse has now progressed this subject, and responded positively to the guidance which has been provided, and has generated two reports to respond to the UK regulatory concerns, and to generate an approach in line with the expectations of the UK SAPs. These documents are 'AP1000 UK Safety Categorisation and Classification Methodology' (Ref. 34), and 'AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components' (Ref. 35).

61 I have reviewed these two documents and consider that Westinghouse has made good progress in this area. I am now satisfied with their safety function categorisation and equipment classification methodology, and application, for the AP1000, from a Mechanical Engineering GDA perspective against SAPs ECS.1 and ECS.2. However, I consider it appropriate to create an Assessment Finding (**AF-AP1000-ME-05**) that this revised methodology should be cascaded through all necessary AP1000 design and safety documentation.

62 I also consider that Westinghouse has recognised the expectation to classify 'duty' system equipment as appropriate, and has reflected this in their classification work to date.

4.2.2 Findings

AF-AP1000-ME-05: *The licensee shall ensure that the appropriate safety function categorisation and equipment classification methodology is cascaded through all necessary design and safety documentation to support the AP1000 Nuclear Power*

Plant (NPP) design. This exercise should specifically include equipment which is the source of postulating initiating events (i.e. safety related systems, also termed duty systems). Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

4.3 Good Engineering Practice

63 I have assessed a number of aspects of the AP1000 against my expectations in relation to Good Engineering Practice. I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle EKP.1 (Ref. 4) states 'The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.'

64 I have specifically selected to sample the following aspects against my expectations of Good Engineering Practice in the nuclear engineering context, during my Step 4 assessment:

- Flexible Connections and Hoses.
- Use of Stellite™ within Mechanical Equipment.
- Pipework Dead Leg Phenomena.
- Mechanical Locks / Interlocks.
- EMIT and System Isolation Arrangements.

4.3.1 Assessment

4.3.1.1 Flexible Connections and Hoses

65 I consider that when comparing a section of pipework to a flexible hose, a flexible hose is a weaker design with lower integrity, with containment properties being of a lower reliability; and their usage typically necessitates an increase in human interactions. I therefore decided to assess Westinghouse's design considerations and criteria for the use of flexible hoses within the AP1000 NPP design.

66 On the topic of flexible connections Westinghouse provided a description of their design associated with the Chemical and Volume Control System, as a suitable example of application of this mechanical equipment.

67 Westinghouse claimed that flexible connections are unavoidable as they support:

- The pressure and leak testing of valves.
- Draining of process lines at low points.
- Venting of process lines.
- Draining and filling of equipment.
- Temporary connection of equipment to support pre-operational activities.

68 The Westinghouse design criteria for flexible hoses are:

- All vent, drain, and test line connections are to contain adequate isolation arrangements, which is an isolation valve located close to the end of the pipe where a blank flange is fitted to the flexible hose connection flange.
- Connecting lines are generally of a 1 inch (25mm) nominal pipe diameter.
- Flexible hoses are specified in accordance with the specification of the connecting pipework.
- Flanged connections are utilised to make the interface; Westinghouse claims this aids access and EMIT.
- The licensee will be responsible for procuring flexible hoses and for ensuring adequate arrangements are in place to ensure flexible hoses are within specification.

I consider these design criteria to be reasonable from a Mechanical Engineering perspective.

69 I am satisfied with the reasoning and explanations provided by Westinghouse from a Mechanical Engineering GDA perspective against SAP EKP.1, on the use of flexible hoses and connections within the AP1000 design.

4.3.1.2 Use of Stellite™ Within Mechanical Equipment

70 The transport of cobalt atoms into fluid systems through either wear, maintenance dressing of sealing surfaces, or corrosion, is a known problem in nuclear power plants, which can lead to high worker dose rates, through the activation of cobalt due to neutron flux within the primary circuit. However, Stellite™, a cobalt chromium alloy, has very favourable mechanical characteristics leading to its use in valve seats, where there is an onerous mechanical duty. I therefore selected to assess and gain an increased understanding of Westinghouse's strategy to control and limit the use of Stellite™ within the AP1000 NPP design.

71 Westinghouse has stated that a review of valve applications had been undertaken for the AP1000 design, which was based on the following criteria:

- Valve function and operating environment.
- Industry reliability performance testing and operating plant experience.
- Manufacturers' fabrication experience and performance history.
- Potential plant operational impact.
- Dose considerations.

72 The following summarises the review recommendations and conclusions:

- Motor Operated Gate and Globe Valves, Stellite™ has been retained for the following reasons:
 - i) Typically open or closed applications (minimal wear).
 - ii) Good maintenance practice reduces particulate mobilisation.
 - iii) Very large investment to date in qualifying existing material pairing.
 - iv) Stellite™ has best friction behaviour for large motorised gate valves.

- 2 inch (50mm) and smaller manually operated globe and check valves, Stellite™ hardfacing has been removed as a specification option, (although limited cobalt is allowed in alternative material options).
- 3 inch (75mm) and larger manually operated gate, stop check, and check valves, Stellite™ is retained as an option, although it has been removed for the bearing pin and bearing blocks for check valves, which was the major area of concern (due to wear for this valve type).
- For butterfly valves, Stellite™ is not a technical requirement, and so has been removed as a permissible option in the specification.
- Air operated globe valves, Stellite™ is retained in the specification, although alternative material pairings are provided as options.
- Pressuriser Spray Valve – a “V” notch ball valve design is utilised, and no alternative material to Stellite™ is available at this time.

73 Through discussion with Westinghouse, I commented that if the specifications allowed alternative materials to Stellite™, and the suppliers were generally able to offer these, then Stellite™ should be removed as a specification option. Westinghouse agreed to consider this. Westinghouse also stated that they were reviewing the valve seat leak criteria with their designers, since they may be over-specifying this parameter as a simple conservative design approach, which then introduces Stellite™ as the only compliant material.

74 Westinghouse TQ-AP1000-677 (Ref.10) response identifies the:

- Specific valves which utilise Stellite™ material.
- Valves containing Stellite™ that are in contact with the primary coolant.
- Arguments and evidence for retaining Stellite™ for specific valve applications.

75 In summary, I consider that Westinghouse has recognised the issues surrounding the use of Stellite™ within NPPs, but I consider that more can be done in this area. I consider it to be an Assessment Finding (**AF-AP1000-ME-06**) that a future licensee retains an active interest in the development of alternative materials to Stellite™ for applications within the NPP domain, and ensures that the final selection of materials for the AP1000 is ALARP in this respect.

4.3.1.3 Dead Leg Phenomenon

76 In recognition that the ‘dead leg’ phenomenon can have detrimental effects on SSCs important to safety, I targeted my assessment in this area to understand how Westinghouse’s design process takes this into account.

77 Westinghouse has explained their design understanding, where ‘dead legs’ are lengths of pipework which nominally contain non flowing fluid (~ water) within the plant primary and other safety important circuits. In their experience such ‘dead legs’ cool down rapidly from the temperature of the main process fluid, and this cooling effect is enhanced by not thermally lagging this section of pipework. However, their understanding in this area has been further developing and improving, and Westinghouse now appreciates that turbulent penetrations of hot fluid occur within ‘dead legs’ to significant depths, as modelled using Computational Fluid Dynamics, and this effect needs to be accounted for in the equipment qualification specifications.

- 78 The design and Equipment Qualification status associated with procurement has limited the visibility of evidence to demonstrate the taking into account of “dead leg” phenomenon for systems important to safety, whilst undertaking the GDA. Westinghouse design process does not apply simple design rules to account for the possibility of turbulent penetrations within dead legs, since the piping layouts are generally scaled up from the AP600 design and then analysed as they stand. Modifications are then made through a general iterative process.
- 79 The response to TQ-AP1000-846 (Ref. 10) refers out to the Thermal Stratification Criteria for the AP1000 (Ref. 78). My assessment has identified that the report was initiated from operational experience of cracking in various NPP piping systems and a number of regulatory bulletins which were issued. The report identifies the criteria considered for the AP600 design, and subsequently for the AP1000 NPP design.
- 80 I consider from my assessment during GDA that Westinghouse’s design process does not stipulate front-end design rules and considerations for the ‘dead leg’ phenomenon in support of developing system pipework arrangements, but rather relies on undertaking an analysis once a design has been developed. In view of the fact that Westinghouse’s understanding of this dead leg phenomenon has further developed and improved, and they apply a confirmatory analysis as part of their process, I consider it appropriate to capture this as an Assessment Finding (**AF-AP1000-ME-07**); the licensee shall provide evidence that they have adequately accounted for the ‘dead leg’ phenomenon in the pipework design of the AP1000.

4.3.1.4 Mechanical Locks / Interlocks

- 81 My assessment also targeted the requirement for an NPP design to include adequate provision for the isolation of process lines to enable Examination, Maintenance Inspection and Testing of plant and equipment to be carried out in a safe and controlled manner. I therefore decided to assess Westinghouse’s design principles and rules for mechanical isolations, locking devices and interlocks. Such features are also important to ensure that correct plant line-up is maintained for normal operation.
- 82 In response to TQ-AP1000-385 (Ref. 10), Westinghouse provided the details of where mechanical locks / interlocks are utilised within the AP1000 design. Westinghouse stated that their valve design specifications place the responsibility for detailed selection (type) and procurement of locking devices onto a future licensee.
- 83 Westinghouse successfully demonstrated the operation of two valves that were fitted with integral key exchange interlocks during a technical meeting in Pittsburgh. The demonstration and the pedigree of the design of interlock were aligned with my expectations.
- 84 My assessment has identified that Westinghouse uses engineering judgement as the principle way of determining if mechanical locks / interlocks are required to be incorporated into the plant design to either support operation process alignment or EMIT isolation. They also use a maintenance validation process, carried out by walking through a system with the aid of a thermal hydraulics simulation model, which takes into account man-machine interfaces.
- 85 In response to my questioning, Westinghouse described a detailed example of a mechanical interlock system, which they described as a ‘defence in depth’ filling sequence of the Passive Containment Cooling Water Storage Tank with water from a fire tender, which is associated with a post 72 hour Design Basis Accident. The detailed

review focused on Process and Instrumentation Diagram APP-PCS-M6-001 and 002 (Ref. 81).

86 I consider the scenario described uses mechanical interlocks to support a process operation and not an expected maintenance activity. The arrangement utilises interlocks to ensure water from the fire tender is routed to a tank in preference to a drain. I advised Westinghouse that I considered the interlocking to be an unnecessary complication for this particular scenario.

87 Westinghouse has also stated that the process design does not incorporate mechanical interlocks that are associated with a Design Basis Accident.

88 I consider the absence of anti-tampering arrangements on manually operated valves to be an area for further justification. Furthermore, Westinghouse has also identified interlock requirements which I consider to be questionable given the nature of the activity. I therefore consider this area to justify an Assessment Finding (**AF-AP1000-ME-08**); a future licensee is to generate their design principles, philosophy, and ALARP arguments to manage the risk of inappropriate tampering of manually operated valves throughout the AP1000 design; whilst ensuring that valves can be operated on demand without unnecessary complication.

4.3.1.5 EMIT and System Isolations Arrangements

89 During Step 4 I identified Westinghouse's proposal to use pipe freezing technology to provide process isolation in support of their planned EMIT regime. I consider this proposal not to be the normal preferred choice for anticipated isolation requirements, but rather a technology utilised to recover from a scenario that has not been generally predicted. I therefore targeted my assessment in this area to further understand Westinghouse's arguments, evidence, and reasoning for adopting this technique. In undertaking my assessment I have used the guidance described within HSG253; The safe isolation of plant and equipment (Ref. 14). Although this document is not directly intended for nuclear application, it represents a useful source of guidance.

90 Westinghouse's response to TQ-AP1000-1062 (Ref. 10) describes their:

- Proposed pipe freeze technology.
- Arguments for selection.
- Reliance on the technology.
- The pedigree of the technology.

91 The AP1000 NPP design incorporates three reactor coolant grade fluid volumes, which are not normally drained and EMIT isolation is proposed to be provided by freezing the applicable pipework arrangement, which are:

- Reactor Coolant System (RCS) components that are positioned below the mid-loop water elevation.
- Spent Fuel Pool (SFP).
- In-Containment Re-Fuelling Water Storage Tank (IRWST).

92 Westinghouse arguments for using the proposed technique is based on the infrequent basis the isolations are required to be made, plus it is dependant on a future licensee's specific EMIT regime, (which is also linked to the limits and conditions, and EMIT identification topic area, RO-AP1000-094).

- 93 Assessment has also identified that isolating the motor operated valve to allow EMIT to be carried out on the 4th Stage Squib valves requires the downstream leg of fluid to be drained by ad hoc means, i.e. splitting of flanges and use of temporary fluid collection containers. In addition the IRWST isolation is provided by a single isolation valve to undertake EMIT of the injection squib valves. The IRWST contains circa 2100m³ of fluid and if the single isolation valve was to fail then a significant hazard would arise. The system design does not have any other provision to contain the fluid within the IRWST.
- 94 I consider that a system isolation first design choice is to provide a suitable valve arrangement, with double valve isolation being provided for systems that are subject to a significant pressure, or temperature, or where there is some other significant hazard e.g. a large volume of fluid is held back. In addition trapped legs of fluid should be provided with an engineered pipework arrangement to allow controlled drainage.
- 95 In summary, Westinghouse's proposal to utilise pipe freezing technology, to provide anticipated system isolation for EMIT activities, has not been justified to be ALARP. I also consider that further justification is required to demonstrate that the system pipework incorporates adequate isolation, and drainage arrangements to enable the anticipated EMIT activities to be carried out in a safe and controlled manner. I consider these subjects to be part of a GDA Issue (**GI-AP1000-ME-03**) concerning system pipework design. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.3.2 Findings

AF-AP1000-ME-06: *The licensee shall review and consider alternative materials to Stellite™ for applications within the NPP domain, and ensure that the final selection of materials for the AP1000 is ALARP in this respect. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-07: *The licensee shall provide evidence that they have adequately accounted for the 'dead leg' phenomenon in the pipework design of the AP1000. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-08: *The licensee shall generate the design principles, philosophy, and ALARP arguments to manage the risk of inappropriate tampering of manually operated valves throughout the AP1000 design; whilst ensuring that valves can be operated on demand without unnecessary complication. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

GI-AP1000-ME-03: *Westinghouse shall provide further justification for the pipework design of the AP1000 for systems important to safety. In particular Westinghouse is required to justify that the AP1000 system designs incorporate adequate isolation and drainage arrangements to enable all anticipated EMIT activities to be carried out in a safe and controlled manner.*

96 The proposed use of pipe freezing technology within the AP1000 design is part of this GDA Issue. Through my assessment, I have also determined that certain proposed isolations rely on a single isolation valve, where I consider failure of this valve would result in a significant hazard. I also consider that Westinghouse shall demonstrate that the associated system pipework incorporates adequate drainage arrangements to enable anticipated EMIT activities to be satisfactorily carried out. In order to address this GDA Issue, Westinghouse shall:

- Generate the arguments and evidence to justify that each isolation that proposes to use pipe freezing technology is ALARP, or satisfy the expectation by alternative means agreed by the Regulator.
- Generate the arguments and evidence to justify that EMIT isolations that rely on a single valve isolation are ALARP, or satisfy the expectation by alternative means agreed by the Regulator.
- Generate the arguments and evidence to justify that all process pipework designs are adequately engineered to provide drainage facilities to enable the anticipated EMIT activities to be carried out in a safe and controlled manner, or satisfy the expectation by alternative means agreed by the Regulator.

4.4 **Metrication**

97 It is the UK Regulator's expectation that an AP1000 built in the UK will be a metric design, including all safety case, design, and supporting documentation, as well as the constructed plant. A cross-cutting Regulatory Observation (RO) was raised to this effect in July 2009, RO-AP1000-038 (Ref. 11). I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle EMT.4 (Ref. 4) states 'The validity of equipment qualification for structures, systems and components important to safety should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.'

A significant concern with the use of non metric equipment in the AP1000 is the susceptibility to maintenance errors, which could degrade the safety of the NPP.

98 This is a cross-cutting RO, affecting a number of assessment disciplines to a greater or lesser degree, but it is particularly relevant to the field of Mechanical Engineering. During the Step 4 process the mechanical assessment discipline has taken the lead in terms of discussing the principles associated with metrication of the AP1000 and establishing the way forward, and then individual assessment disciplines have reviewed the output from this process as applicable to their individual areas, and drawn conclusions as appropriate. The discipline specific assessments and conclusions are reported in individual assessment reports as necessary.

4.4.1 **Assessment**

99 Westinghouse provided an initial response to the RO in December 2009. This comprised document reference APP-GW-G1-011, AP1000 Standard Plant Metrification (Ref. 85); (noting that 'metrication' and 'metrification' are considered to be equivalent). This initial cross-cutting response was not considered to be adequate and subsequent discussions were held during the Mechanical Engineering technical meeting in Pittsburgh in February 2010.

- 100 Prior to this meeting, I issued further guidance to Westinghouse regarding the application of metrication to the AP1000, which had been developed internally through cross discipline discussion with GDA colleagues and management. This guidance is stated as follows:
- For construction of the AP1000 in the UK, the regulatory expectation is that the design and associated equipment should be fully metric (i.e. conceived, designed, and manufactured as metric); or as an alternative, 'quasi metric' (i.e. initially conceived as imperial, but now designated and designed as metric using metric codes / standards, and fully dimensioned as metric). All fastenings shall be metric.
 - However, exceptionally, the Regulator may accept non-metric products (including fastenings) for one-off fabrications of a specialist nature associated with the Nuclear Steam Supply system (NSSS), or other specialist NSSS equipment, but these will need to be justified to the Regulator on a case by case basis.
 - Notwithstanding the above, all design and safety case documentation shall be fully metric from conception, through intermediate results, to final presentation.
 - All information displayed within the constructed facility will need to be fully metric.
- 101 This guidance was subsequently confirmed to Westinghouse by letter, reference WEC70154R, dated 17 March 2010 (Ref. 16).
- 102 During the February 2010 meeting, and to move the RO resolution forwards, Westinghouse stated that the design work was in fact undertaken in dual units; except that safety analysis work was done in imperial units and converted to metric at the end, for historical reasons. Westinghouse stated that the associated software contained embedded imperial units, and they had a concern that converting this analysis software into metric would introduce a risk of error.
- 103 I commented in response to Westinghouse that construction and subsequent maintenance / modification of the AP1000 were the focus of ND's cross-cutting concerns in this area, and these concerns were safety based, and based on UK Operational Experience.
- 104 Westinghouse stated that they are producing a full set of metric drawings for their China project, and some were tabled for review.
- 105 Westinghouse stated that their goal was 70% localisation for the AP1000 global design, and therefore notwithstanding this RO, they expected most components for the UK to be delivered to metric standards.
- 106 I stated that the design should lead procurement in relation to this matter, and not vice versa which ND had inferred from WEC's response to the RO to date. Westinghouse indicated they understood this point. I also stated that the UK AP1000 should be a metric design, with imperial elements / aspects by exception, and specifically justified as necessary. Westinghouse indicated they understood this point. I advised that the justification for any retained imperial products, documents and / or processes, would be reviewed by the relevant ND assessment discipline.
- 107 Westinghouse provided a revised response to the RO in April 2010, which included provision of an updated version of APP-GW-G1-011 (Ref. 86). This documentation was discussed during the subsequent Mechanical Engineering technical meeting in Pittsburgh in May 2010, described as follows.
-

- Westinghouse provided information in respect of recent progress regarding the RO on metrication. I commented that ND had recently received a further response to the Regulatory Action associated with this RO, and I was encouraged that Westinghouse had understood and adopted the principles as explained in the recently provided guidance in this area. I also explained that this was a cross-cutting topic area, and although the mechanical discipline had taken the lead in terms of metrication philosophy, Westinghouse should pro-actively engage with relevant assessment disciplines to gain agreement as to whether the approach, and specifically list of exceptions, is acceptable in their areas.
- Westinghouse described their proposed justification approach where they did not propose to adopt metric units, as follows:
 - i) Issue – what prevents the adoption of metric units
 - ii) Impact – what are the consequences of not adopting metric units
 - iii) Solution – how are the consequences mitigated.

I commented that this approach appeared rational and pragmatic.

108 The meeting reviewed a preliminary list of metrication exceptions, and I identified the assessment disciplines which took the lead in these areas, for Westinghouse's coordination.

109 In respect of Mechanical Engineering assessment, I provided the following advice:

- Piping should be listed and analysed / justified as a separate grouping to permanent civil structures.
- CRDMs were a reasonable candidate as a metrication exception.
- Lifting equipment should be identified individually, and it would be difficult to justify equipment as exceptions where it was not closely linked to the NSSS.
- Squib valves are a reasonable candidate as a metrication exception.
- Turbine parts would be difficult to justify as metrication exceptions.

110 In September 2010 Westinghouse issued an updated version of APP-GW-G1-011 (Ref. 87), which was discussed during the technical meeting held in Pittsburgh during the month. During this meeting, the following points were made:

- Westinghouse presented the latest response to the Metrication RO, Document titled Standard Plant Metrication, APP-GW-G1-011, Rev. 2, dated September 2010. The discussion focussed on the appendix which details the exceptions to (quasi) metrication, which was intended to be in line with guidance provided to Westinghouse earlier in the year. I stated that a number of areas are for other disciplines to assess, and Westinghouse has written to ND requesting a formal response to the document in early October. However, from a Mechanical Engineering perspective, I stated that I was not content with general flange bolting being an exception to metrication, nor was I content with the light and heavy load handling systems being exceptions. I also stated that the exceptions list should be explicit and complete, and it would also assist if Westinghouse described in general terms the plant and equipment which would be provided in metric, to put the metrication exceptions into context.

- I stated that I would provide a more considered response following assessment in the UK, and this response would be incorporated into the cross-cutting letter to be provided by ND, but I indicated my initial disappointment with the Westinghouse response.

111 ND subsequently wrote to Westinghouse in early October 2010, reference WEC70243R (Ref. 17) , to formalise the assessment view across relevant disciplines, and the Mechanical Engineering aspects of this response are detailed as follows:

- Permanent Structures (piping, flanges, valves and bolting): the proposal is not acceptable, since it includes wide-scale use of imperial bolting / fastenings. We questioned Westinghouse on the policy for pipe supports and other Small Part Steelwork, and they were unclear in this area (but suggested the fastenings here may also be imperial, which again would involve wide-scale use of imperial fastenings). We also questioned the arrangements for the ventilation equipment; although not explicitly stated as an exception Westinghouse were somewhat unclear in their response. We commented that the exceptions list should be explicit and complete; everything else will be metric / quasi metric, with metric fastenings. We advised that Westinghouse should generally describe the equipment which is metric as background information to help provide greater clarity, without undermining the fact that the exceptions list should be complete, everything else is (quasi) metric by default.
- Design analysis: we had a lengthy discussion in this area. Although we stated that we accept that existing, complex codes utilised imperial inner 'workings', and as such the input and output could be converted to metric, for any future design work associated with installation design, (e.g. pipe loadings etc), then the work should be undertaken fully in metric. Westinghouse stated that much of the design work is already complete, and so this would not apply; however I am not convinced here since much detailed design work will be associated with mechanical installation following award of contracts etc.
- Control Rod Drive Mechanisms: we stated that we would review the response in detail, but are now content with this equipment being an exception to metrication, except that the interface with lifting equipment will need to be specifically controlled.
- Integrated Head Package: we stated that we would review the response in detail, but are now content with this equipment being an exception to metrication, except that the interface with lifting equipment will need to be specifically controlled.
- Squib valves: we stated that we are content with the squib valve internals etc being imperial, including thread forms, but the connecting flanges should utilise metric fastenings.
- Light and heavy load handling systems: this category groups a large number of lifting equipments together which we advised is not appropriate. Although we would accept structural shapes as being quasi metric, all fastenings should be metric, and so we stated that we were not content with the Westinghouse response.

112 The subject of metrication was discussed again from a Mechanical Engineering perspective in December 2010 at the final Mechanical Engineering assessment meeting in Pittsburgh. Subsequent to the meeting Westinghouse issued a further update to document APP-GW-G1-011, now at Rev 3, AP1000 Standard Plant Metrication (Ref. 18).

- 113 In particular, for the following cranes, Westinghouse has now made the following commitments:
- Polar Crane: fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - Cask crane: fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - Equipment Hatch hoist (two off): fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - Re-fuelling machine: a number of components will be specifically procured as metric equipment for the UK, and fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - Fuel Handling Machine: a number of components will be specifically procured as metric equipment for the UK, and fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - Fuel Transfer System: a number of components will be specifically procured as metric equipment for the UK, and fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - New Fuel Elevator: a number of components will be specifically procured as metric equipment for the UK, and fasteners that are used to secure components and / or assemblies that would need to be replaced or serviced during the life-cycle of the equipment will be metric fasteners.
 - All other cranes within the UK AP1000 will be fully metric.
- 114 In summary, I consider that Westinghouse has made significant progress in this area, in terms of accepting the principles of metrication as described in the guidance provided by ND across all discipline areas, and in terms of applying these principles to Mechanical Engineering. Nevertheless, there still remain residual concerns with the final position reached with Westinghouse during Step 4, specifically relating to flange bolting, and fasteners associated with engineered connectors. Some further clarification is also appropriate in respect of design analysis. For this reason I have decided to capture this within GDA Issue (**GI-AP1000-ME-02**) for Mechanical Engineering. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.4.2 Findings

GI-AP1000-ME-02: I consider the following to be a GDA Issue:

- *The Guidance to Requesting Parties requires that documents submitted for GDA use SI units. As a corollary it is the expectation that the design submitted by the Requesting Party is essentially metric, using metric Structures, Systems and Components. HSE-ND has provided advice in March 2010 to*

clarify the detail of their expectations, and to allow variation from this expectation for a limited, controlled, and justified sub set of equipment.

- *To date, HSE-ND does not consider that Westinghouse has satisfactorily met this expectation for Mechanical Engineering equipment and associated systems.*
- *This is a cross-cutting subject, although this report describes the Mechanical Engineering aspects of this GDA Issue.*

115 In particular I consider the following to be the outstanding matters associated with Mechanical Engineering which require resolution through this GDA Issue:

- Permanent Structures (piping, flanges, valves and bolting): the proposal is not acceptable, since it includes wide-scale use of imperial bolting / fastenings. Furthermore the exceptions list should be explicit and complete; everything else will be metric / quasi metric, with metric fastenings. Westinghouse should generally describe the equipment which is metric as background information to help provide greater clarity, without undermining the fact that the exceptions list should be complete, everything else is (quasi) metric by default.
- Design analysis: Although I accept that existing, complex codes utilise imperial inner 'workings', and as such the input and output could be converted to metric, for any future design work associated with installation design, (e.g. pipe loadings etc), then the work should be undertaken fully in metric.
- Squib valves: I am content with the squib valve internals etc being imperial, including thread forms, but the connecting flanges should utilise metric fastenings.

116 I consider Westinghouse shall undertake the following action to progress and respond to this GDA Issue:

- Provide an updated response to document titled 'AP1000 Standard Plant Metrication, APP-GW-G1-011', to reflect the guidance provided by ND, and the comments provided in the letter dated 11 October 2010 for mechanical equipment, and subsequent discussion held in Pittsburgh in December 2010. Westinghouse should commit to re-designing equipment in line with the guidance, or provide a much more rigorous justification (which aligns with the guidance provided) as to why they consider equipment should be an exception to metrication, or satisfy the expectation by alternative means agreed by the Regulator.

4.5 Limits and Conditions and EMIT Identification

117 A key feature of a safety case is the identification of the limits and conditions which define the safe operating envelope for plant operation. In the UK these limits and conditions are termed Operating Rules and are regulated through Nuclear Site Licence Condition 23. Although making and implementing the arrangements associated with Licence Condition 23 (LC 23) is the responsibility of a future licensee, it is important that sufficient information has been generated through the safety case documentation suite to facilitate this, and it is also important that the Responsible Designer (Westinghouse) recognise this requirement, and will in future support a licensee by providing appropriate technical information and support.

118 In a similar fashion, a key feature of a safety case is also the identification of Examination, Maintenance, Inspection and Testing requirements for the Structures, Systems and Components (SSCs) within the Nuclear Power Plant. In the UK these are

regulated through Nuclear Site Licence Condition 28 (LC 28), which includes the requirement to generate a Plant Maintenance Schedule to define the safety important maintenance activities, with appropriate periodicities.

- Safety Assessment Principle SC.6 (Ref. 4) states 'The safety case for a facility should identify the important aspects of operation and management required for maintaining safety'.
- Safety Assessment Principle EMT.1 (Ref. 4) states 'Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.'

4.5.1 Assessment

119 During the initial Step 4 Mechanical Engineering technical meetings I provided a background to the mechanical assessment in this area, in that Operating Rules as described by LC23 are a key area from translating safety case requirements into the operating plant regime and associated regulatory compliance inspection process. I stated that this was a cross-cutting issue of interest to all assessment disciplines, but that the ND Division 1 licensing team would be providing more guidance specifically on licence conditions.

120 Westinghouse explained their proposals in this area, which described their 'Tech Spec' arrangements, which are expected to be the equivalent to those for UK plants that are based on Westinghouse designed Pressurised Water Reactors (PWRs), i.e. Sizewell B.

121 The 6 Generic Operating Modes of the AP1000 are as follows:

- Mode 1 – Power Operation.
- Mode 2 – Start-up.
- Mode 3 – Hot Standby.
- Mode 4 – Safe Shutdown.
- Mode 5 – Cold Shutdown.
- Mode 6 – Re-fuelling.

122 The Tech Specs specifically identify mode applicability and plant configurations, and for described Conditions, identify Required Actions and associated Completion Times. They also identify specific Surveillance requirements with associated periodicities. Westinghouse identified the number of Tech Specs considered likely to be associated with each plant area, e.g. the Reactor Coolant System has 17 Tech Specs.

123 As part of my Mechanical Engineering assessment, I have also reviewed the accessibility and practicability for maintenance of mechanical equipment on a sampled basis as I have discussed various equipment types, and also discussed the typical maintenance which is undertaken during the lifetime of the NPP. This is discussed as necessary within the relevant sections of this report.

124 Through discussions with Westinghouse, and liaison with my assessment colleagues, a cross-cutting Regulatory Observation was raised to cover this subject area, RO-AP1000-094 (Ref. 11), in order to require Westinghouse to develop a coherent and consistent philosophy across all assessment disciplines.

125 Westinghouse has now produced an initial response to this RO, dated January 2011 (Ref. 11). I have reviewed this document from a Mechanical Engineering perspective, and consider it falls significantly short of my expectations in terms of depth of content, and also coherence with other parts of the Westinghouse safety justification which has

been developed for the UK. HSE-ND has written to Westinghouse on 14 January 2011, (Ref. 33), to state that the response falls short of our expectations. This subject is now being taken forward as a cross-cutting GDA Issue, **GI-AP1000-CC-01** (Ref. 107).

126 In order to resolve this subject from a Mechanical Engineering perspective, I consider that Westinghouse needs to develop a more substantial response, which should specifically cover the following areas:

- All Mechanical Engineering items which attract a safety classification in line with UK expectations should be considered in terms of their EMIT requirements, and whether these requirements are directly driven by the safety case (Design Basis Analysis (DBA) and /or PSA), or are based on manufacturer recommendations, or plant operating experience, or OEF considerations (or appropriate combinations)).
- All Mechanical Engineering items which attract a safety classification in line with UK expectations should be considered in terms of their association with plant limits and conditions, to ensure that any such limits and conditions for these items are adequately recognised and documented. Westinghouse should also recognise that these limits and conditions should also correlate to EMIT requirements, (for example in terms of limitations on taking equipment out of service for maintenance).

I recognise that the responsibility for making and implementing adequate arrangements in respect of LC23 and LC28 will rest with a future licensee, nevertheless I consider that Westinghouse should generate a sufficient depth of information to facilitate this process, and should clearly identify the links to the safety case assumptions in this respect.

4.5.2 Findings

127 My Mechanical Engineering finding in this area is being taken forwards as a cross-cutting GDA Issue, **GI-AP1000-CC-01** (Ref. 107).

4.6 Codes and Standards

128 My assessment of codes and standards identified that Westinghouse froze their codes and standards selection on the first licensing of the AP1000 nuclear power plant design in the US.

- Safety Assessment Principle ECS.3 (Ref. 4) states 'Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.'

129 As part of my assessment I intended to gain an increased understanding of the changes to applicable codes and standards since the design freeze, with specific aspects of interest being:

- Identification of the codes and standards that have been the subject of a change.
- Assessment of the impact of the identified changes.
- Arguments as applicable for the AP1000 codes and standards not being updated to the latest version.

130 To address this line of enquiry, Westinghouse has decided to carryout a codes and standards gap analysis. This is to generate the arguments and evidence that their proposed codes and standards are adequate and consistent with UK and international

good practice, and are appropriate to support the design, construction, manufacture and operation of an NPP within the UK.

4.6.1 Assessment

131 During a technical meeting held in Pittsburgh in December 2010, Westinghouse stated that they have not as yet completed this task (gap analysis). During this meeting they explained their proposed methodology for moving forwards to completion.

132 The initial report, UKP-GW-GL-045, was generated by a contractor and it was Westinghouse's view that it did not meet expectations. As a consequence the document is now the subject of an update.

133 Westinghouse stated their objective is to deliver a report that assesses the codes and standards utilised within the AP1000 design against the UK and European regulatory expectations for modern nuclear power plants. The report is to include the arguments and evidence that support the fundamental claim that the AP1000 codes and standards are appropriate to support the design, construction, manufacture, and operation of a nuclear power plant within the UK.

134 The claim is supported by two principle arguments:

- The AP1000 codes and standards are adequate and consistent with UK and international good / best practices.
- The versions of the design codes utilised within the AP1000 nuclear power plant design are adequate, when compared to more recent versions of the same code.

135 A graded approach is being adopted to develop the arguments and supporting evidence. This is in line with the guidance provided within the ND SAPs and TAGs. i.e. the higher the safety importance, the more detailed the justification shall be. Thus their first task is to organise the codes and standards in order, relative to their safety significance. This strategy should also make the audit trail visible and transparent.

136 Through undertaking this exercise, Westinghouse has identified some inconsistencies, and intends raising a class 1 DCP to reconcile the situation. In addition they have only gone up to 2008, as the effective start of GDA, since they consider it reasonable to have a design freeze for GDA in this respect. Whilst recognising the concept of a design freeze, I commented that through their normal process they should keep abreast of developments re codes and standards and any significant engineering implications.

137 The gap analysis does not include:

- Codes and standards that do not support items important to safety.
- Electrical codes and standards, which are addressed separately.
- Control and instrumentation codes and standards, which are also addressed separately by analysis supporting the PCSR.

138 To date this exercise had identified no impacts for the AP1000, (although Westinghouse stated that a plant designed to the latest codes and standards may be slightly different in some aspects).

139 In summary, although I have not as yet seen the final product, I consider that the process appears to be rational and comprehensive.

140 To progress this line of enquiry, I consider that Westinghouse is required to complete the scope of work and issue their revised codes and standards report for further assessment,

(as considered necessary), which I consider to be an Assessment Finding (**AF-AP1000-ME-09**).

141 In addition, I consider it to be an Assessment Finding (**AF-AP1000-ME-10**) that a future licensee retains an active interest in changes to applicable codes, standards and UK legislation.

4.6.2 Findings

AF-AP1000-ME-09: *The licensee shall ensure that evidence is generated to ensure that the proposed codes and standards for the AP1000 are adequate to support design, procurement, installation, operation, and subsequent EMIT activities. The licensee should also ensure that the AP1000 codes and standards meet applicable UK Health and Safety legislation, including regulations and ACOPs (as appropriate). Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-10: *The licensee shall make and implement adequate arrangements to ensure the AP1000 NPP design for the UK recognises as necessary changes to applicable codes, standards, and legislation. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.7 Control Rod Drive Mechanisms

142 As part of my Step 4 assessment, I have continued to target the evidence that supports the design of the Control Rod Drive Mechanisms (CRDM) due to their safety role in reactivity control and their revised safety claim of being able to successfully carrying out 6 million operational steps. I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle EAD.1 (Ref. 4) states 'The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.'
- Safety Assessment Principle EMT.1 (Ref. 4) states 'Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.'
- Safety Assessment Principle EQU.1 (Ref. 4) states 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'

143 To achieve my assessment objectives, I targeted:

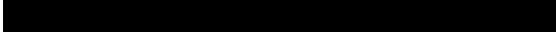
- Westinghouse's CRDM Life Time Test.
- The derivative issue relating to shim safety functional performance.
- The CRDM safety classification.

4.7.1 Assessment


4.7.1.1 CRDM Life Time Test

144 Westinghouse has recently undertaken and completed a CRDM life time test, which was driven by the 60 year design life of the AP1000 NPP and the operational desire for a CRDM to successfully carry out 6 million steps. Historically, CRDMs have been used in baseload power plants that stay at full power between refuelling with core activity being controlled by the chemical control systems. These conditions have typically led CRDMs to accumulate less than one million steps over their forty year design life. The AP1000 is designed to have a greater capability to adjust power by using its reactor control rods, and hence an increased CRDM stepping design requirement.

145 The principal aim of the test was to provide the evidence that the proposed design is able to achieve its design intent and with adequate margins.

146 The CRDMs satisfactorily completed 8.25 million steps, prior to the test being stopped. The trials tested two design configurations. 

147 Assessment of APP-MV11-T2-021 Rev A Engineering Summary Report for the AP1000 Control Rod Drive Mechanism (CRDM) Model L106AP Life Test (Ref. 73) identified:

- Some of the stainless steel ASTM A240 304 shims incorporated into the design to establish a non-magnetic gap between the electromagnetic poles within the latch assembly suffered circumferential cracking on inspection at circa completing three million steps.
- At six million cycle steps a number of cracked shims were replaced with  shims.

148 The latch mechanism (Figure 1) contains stainless steel shims, which are located between the magnets with their purpose to provide an insulation barrier between the different magnetic fields. The life time test found that a number of shims contained cracks and one shim was found to have split into two. However, Westinghouse claimed that the assembled tolerances of the latch assembly retain the shims in situ.

149 Westinghouse subjected the CRDMs to just over eight million steps, and has made a six million cycle claim on the CRDMs in terms of design life. I consider in principle this represents an acceptable margin. However, based on the above evidence associated with the shim performance, and the fact that the replacement shims were only subjected to the order of two million steps, my regulatory judgment is that there was a significant shortfall in the evidence for a six million step claim.

150 The test loop configuration comprised a four unit set up and out of the 4 station set-ups only stations 2 and 3 had their lift shims changed at the 6 million step inspection. Westinghouse's arguments for only changing the lift shims were principally due to ease of access, and limiting the amount of equipment requiring disassembling.

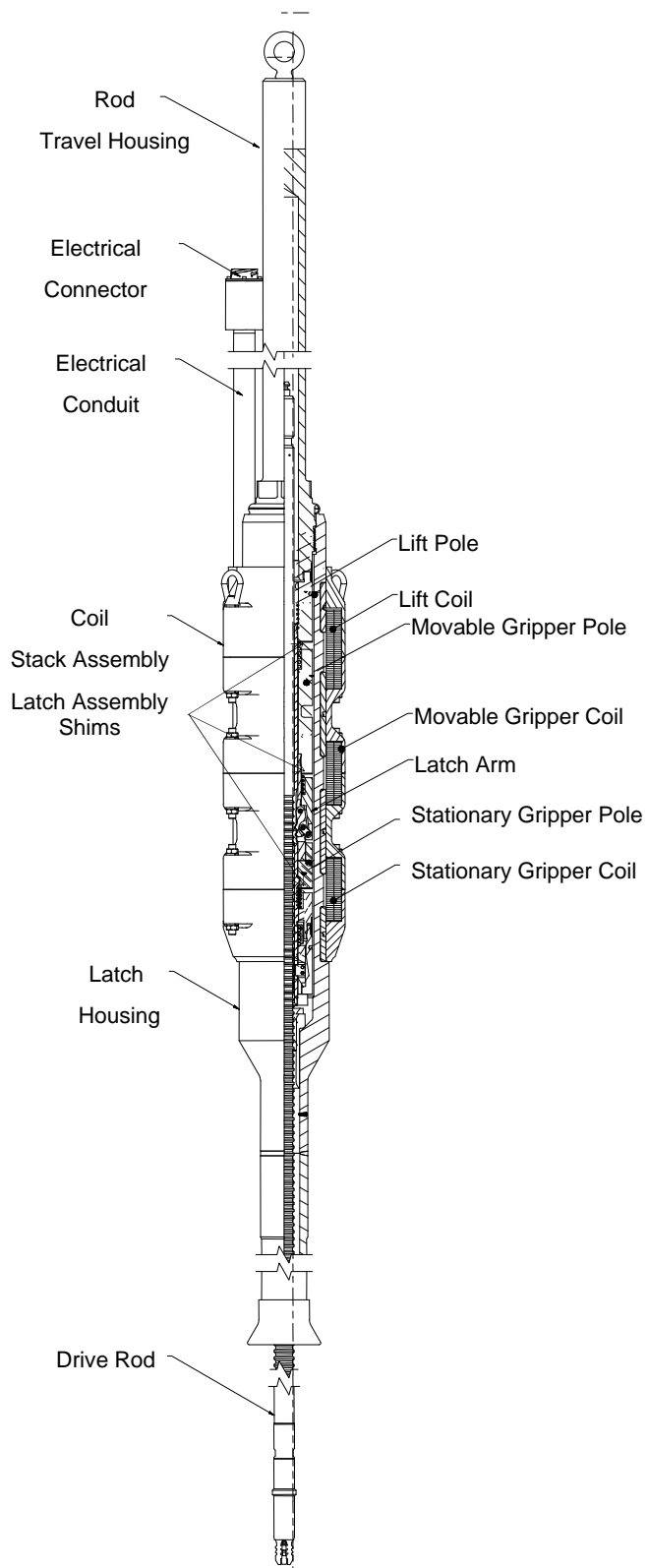


Figure 1
CRDM - Latch Assembly Arrangement

- 151 Westinghouse has confirmed that the selected shim material is [REDACTED], they have no plans to carry out any additional life time tests for the CRDMs, and the [REDACTED] shims at the time of carrying out the Life Time Test had not been subjected to any detailed metallurgical analysis (in terms of material testing or microstructure examination).
- 152 They clarified that each CRDM latch assembly has a design life of sixty years, or performing 6 million steps. I consider from a UK regulatory perspective this criteria forms a safety claim.
- 153 My assessment has also identified that the life test included a number of control rod drop tests. The CRDM Latch Assembly Life Test Specification (Ref. 75) specified the test parameters. I have assessed the results which provide the evidence that the design criteria were achieved, and which are collated within the Test Report for Production Life Testing (Ref. 91). I am now satisfied in this respect.
- 154 In summary, I considered I had identified a shortfall in evidence in support of Westinghouse CRDM claim. As a consequence, I generated and issued Regulatory Observation RO-AP1000-069 (Ref. 11); Equipment Qualification CRDM Shims.

4.7.1.2 Shim Safety Functional Performance

- 155 In response to my line of enquiry Westinghouse made the following claims, which I have commented on as part of my assessment activity:
- Shim cracking in no way hinders the functionality of the latch assembly. I judged this to be unsubstantiated at the time. My judgement was based on consideration of the small sample size of 4 units tested, and the fact the design criteria of being functional for 6 million steps was outside previously well understood and substantiated design parameters for a CRDM.
 - Loose particles are restrained in position; both by the small tolerances associated with the pressure boundary housing and internally by a physical barrier between the shim and the clearance void around the control rod.
 - Test and operational experience of CRDMs shows that there is no detectable deterioration in performance over the operational life; until the end of life is approached when the rods start to miss steps (due to wear), which is detectable. I consider this provides regulatory confidence in the CRDM design principle, in that there is a gradual and detectable degradation in performance towards end of life.
 - A potential cause for the circumferential cracking is the impact loads of the stepping sequence being in excess of the 304 Stainless steel yield strength. The [REDACTED] [REDACTED] has a higher yield strength and subsequently does not yield under stepping action. At the time I considered Westinghouse needed to increase their understanding in this area, and provide evidence of why the 304 stainless steel material suffered circumferential cracking, and that this fault would not occur for the replacement [REDACTED].
 - They selected to perform a detailed calculation of the impact loads on the [REDACTED] shim material to confirm that it is an improvement to the 304 Stainless steel shim material, and is adequate for its duty.
- 156 My expectation was for Westinghouse:
- To focus on providing evidence that the [REDACTED] material, which is now the GDA reference design for the shims, is adequate for the 6 million step claim,

either with empirical or theoretical data, or a combination of the two. Claiming circumferential cracking does not impact the functionality of the equipment and has no safety consequence should not be a principal claim, but may aid a defence in depth type argument as a secondary claim.

- Understand the impact of changing the shim material, and ensure it does not have a detrimental impact on other aspects of the design that affects the CRDM design intent.

157 Technical discussions confirmed the shims' role is to ensure a rapid response is achieved in the stepping of a control rod, which is up to 72 steps per minute. This supports my judgement of the shims' important safety role within the whole assembly.

158 Westinghouse advised that they have only carried out four life time tests since 1969. They confirmed that a life time test is only carried out when there is a fundamental change to the design parameters e.g. the move to a 6 million operational step requirement.

159 Previous tests focused on operability and not the CRDM condition, although significant shim impact (brinelling) was noted during the original 2 million step life test in 1969.

160 Westinghouse has provided some operational feedback on shims. Combustion Engineering San Onofre Nuclear Generating Stations had evidence of a shim break in 2009, which had been in service for 26 years and WEC Technical Bulletin TB-09-3 covers the subject. Westinghouse identified that the cracking never affected the ability of the CRDM to release the control rod (although the CRDM incurred some erratic stepping). The shim failure was attributed to the failure of some tack welds, which initiated cracking in the shim. Westinghouse stated that their design is very different, it does not contain any tack welds and QA for the AP1000 products is in place from the initial procurement of material, which was not the case for the early CRDMs.

161 Westinghouse has clarified:

- The life test provides evidence that a cracked shim does not impair stepping sequence. However it can be postulated that a displaced shim has the possibility of leading to an erratic operation and lead to miss-stepping. An erratic operation may result in a non operational CRDM, which could be replaced during a subsequent outage.
- A cracked shim does not get displaced or impair the latch functionality and is unable to migrate from its closed gap due to the clamping action that holds it in place, therefore not impairing the ability to drop a Rod Cluster Control Assembly (RCCA).
- The life test provides adequate evidence to support their claim on achieving CRDM functionality, which demonstrated the:
 - i) ability to step (raise or lower) a drive rod;
 - ii) ability to hold a drive rod in position;
 - iii) ability to release the drive rod within 150 milli seconds.

162 They explained that a number of parameters utilised for the life test exceeded the normal operating parameters. I consider carrying out a test with conservative parameters is good engineering practice. Westinghouse advised that operating the life test at higher temperatures results in lowering the coolant viscosity, which increases the speed of the impacting pole faces. In addition the higher temperature reduces the shim material yield strength. I also noted from discussion that the test rig loop contained excess debris,

which Westinghouse considered had a detrimental (and hence conservative) impact on component wear.

163 I noted from discussion that:

- The intent for carrying out the life test was to determine the assembly life expectancy.
- Non Destructive Examination of the [REDACTED] shim did not identify any signs of cracking following the completion of 2.25 million steps.
- The design weakest point from a functionality perspective is the latch to pin joint.
- Westinghouse claimed the shim is not the weakest point in the design, therefore they consider the life expectancy of the assembly is not affected by material change of the shim.
- [REDACTED]
- There is no change in loading conditions due to the new shim material.
- There is no change in the way the latch assembly functions due to the new shim material.
- Westinghouse engineering judgement, peer review of the material, and tests to date demonstrates the shim will function satisfactorily.
- They also consider there is no requirement to carry out a further life time test, the existing test results remain valid as the change in the shim material does not impact the life and functionality of a unit.
- A Failure Modes and Effects Analysis (FMEA) (Ref. 74) has been carried out, providing some evidence that no postulated CRDM latch assembly failure prevents the latch assembly to release or lower the control rod, or cause it to inadvertently be raised or withdrawn. This is also consistent with operating experience.
- The rod control system incorporates a step counter, which allows each unit to be monitored during their operational life and for the appropriate EMIT requirements to take place.
- There are no credible failure mechanisms that would cause the rods to lose their safety function, (i.e. would cause them to fail to drop).

164 On the subject of identifying the triggers that would evoke an additional life time test requirement, Westinghouse has advised:

- A life test is implemented as judged necessary to ensure the product functions as intended and to increase the understanding of operating characteristics and failure modes of a unit.
- To validate design changes that are judged to impact functionality e.g. moving parts, re-design (dash pots eliminated) etc.
- To qualify and verify design changes to improve a unit life e.g. double tooth latch arm, locking sleeves, pin design etc.

165 During discussions Westinghouse has stated:

- The CRDM design life of achieving 6 million steps was selected on commercial grounds. Each unit is of a design that allows the latch mechanism to be replaced in position with the aid of dedicated equipment. The radiation dose uptake in replacing a

CRDM latch assembly is relatively low due to the task being carried out by remote means. A dedicated tool is attached to the Polar Crane auxiliary hoist, which is then lowered and is then attached to the CRDM rod travel housing. The tool then remotely cuts the seal welds of the pressure boundary. The latch unit assembly is then able to be raised and removed from the CRDM. A replacement latch assembly unit is then fitted following a reverse sequence.

- In operation each CRDM is continuously monitored with drop tests carried out on a routine basis. On this basis I consider any decrease in functionality is able to be identified in sufficient time and the appropriate action taken.

166 It is my expectation that during the plant operational life of a NPP the EMIT requirements specify an inspection of shims is carried out and observations recorded following the replacement of a latch assembly. Adoption of this expectation also provides Westinghouse an opportunity to implement a bench marking process for the future fleet of the AP1000 NPPs.

167 At a technical meeting Westinghouse explained their initial submission response against RO-AP1000-069 Equipment Qualification (Ref. 11).

168 Following discussion, I clarified that my expectation is that the safety claim is structured as follows:

- Primary claim: analytical and empirical evidence shows that an [REDACTED] shim is not the subject of cracking up to 2.25 million steps.
- Secondary claim: analytical evidence shows that an [REDACTED] shim is very unlikely to be the subject of cracking prior to completing 6 million steps.
- Tertiary claim: shim cracking does not hinder the functionality of a latch assembly.

169 Westinghouse has described in detail their arguments and evidence in support of their tertiary claim on the CRDM latch mechanism, which is “shim cracking does not hinder the functionality of the latch assembly”.

170 They explained that if a small fragment fractures off a shim, it could be considered possible for it to migrate into the clearance gap between the latch assembly outside diameter and the latch housing inside diameter. This could potentially result in an ineffective latch assembly load transfer or lift function. However it is not possible to hinder the dropping of a control rod. For this to occur a large piece of debris would have to lodge precisely behind the latch arm or above the latch link while the latch is engaged in the drive rod. It is considered the radial clearance, a nominal 3.3 mm gap between the latch assembly and housing, prevents this. In addition the latch opening force of 1500 N is considered sufficient to overcome any resistance offered by a fragment and would deform it sufficiently to enable a control rod to be dropped, which is achievable when the gap is restricted by up to 27%.

171 Westinghouse has now re-issued their RO response that captures the arguments and evidence discussed above. In summary, I now consider on balance that the Westinghouse issued response under correspondence DCP_JNE_000514 (Ref. 66), which includes the updated document APP-MV11-T2-021 Rev 0, meets my expectations and provides sufficient arguments and evidence to support Westinghouse’s claim that the CRDM is of a design that has been adequately evaluated and tested to meet its design intent. However, Westinghouse has not provided complete arguments and evidence to support their defence in depth tertiary claim, specifically that debris migrating between the latch assembly outer diameter and the latch housing inner diameter does not impair a latch from opening on demand. Nevertheless, giving due consideration to the claim

weighting, being proportionate, and noting that the mass of the control rod assembly aids a latch assembly to open on loss of the coils magnetic field, I do not intend to pursue this aspect any further.

172 I consider Westinghouse's proposal to update the CRDM Operational and Maintenance manual so that a future licensee carries out inspections of the shims during the NPP operational life, which is being implemented under the Westinghouse Corrective Action Process (CAP), to be an Assessment Finding (**AF-AP1000-ME-11**). In clarification, my expectation is that visual inspection of a CRDM shim should be carried out following the replacement of a latch assembly, and not as a routine scheduled maintenance inspection requirement; a future Licensee should ensure that the EMIT requirements take into account my expectation.

4.7.1.3 Safety Classification

173 My Step 3 assessment judged the CRDM latch assembly as being important to safety and I considered the assembly is required to be allocated with the appropriate safety classification. Westinghouse agreed with this consideration, and advised that a design change had been raised and was going through Westinghouse's design change process.

174 Through requesting evidence of this design change, I identified that the Project team was now challenging the design change. I considered this to be of regulatory interest and decided to target this aspect.

175 Westinghouse explained the design change that supported the safety categorisation of the latch mechanism is assigned with a Class 3 status, which is assigned to a change with no interfaces with other disciplines, and is of a value less than \$25K; (typically comprising a typographical error). My initial regulatory expectation was an assignment of Class 1 in this case, due to the proposed change affecting a component's safety classification. My earlier assessment had also identified that the CRDM specification text varied within sections, with some sections classifying the latches and others not. The DCP was being processed assuming the non classification was a typing error, and all other safety supporting documentation was correctly classifying the latch mechanism. My regulatory expectation in this scenario is to assume the bounding case, which is again assignment of a Class 1 status to the DCP. In addition Westinghouse proceeded to clarify that a QA Corrective Action Process system exists within the organisation to capture non compliance aspects. Westinghouse confirmed that a CAP had been raised against the subject in question and was going through its process steps. The CAP challenges the assignment of Class 3 to the above DCP, and if it is found that the challenge is correct, then a new DCP will be raised to re-classify the original DCP to a Class 1.

176 In summary, I consider my sample assessment identified a shortfall in the application of the DCP process. In parallel, an individual member of the Westinghouse design team had initiated the issue of a QA CAP to review and correct the shortfall.

177 From discussion, it was apparent that the issue related to the original US classification methodology and with Westinghouse now adopting a specific safety classification methodology for the UK, I therefore decided not to pursue the line but to target the UK specific classification.

178 Discussions targeted the AP1000 UK safety categorisation and classification methodology to the CRDM and its subcomponents. I noted that a number of subcomponents remain classified as 'non safety'; for example the guide sleeve and the rod travel housing eyebolt. My expectations are these two items are assigned with the

appropriate safety classification as they are items important to safety. The guide sleeve provides guidance for ensuring a control rod assembly is positioned in its appropriate position to control the reactor reactivity; the eyebolt is utilised during a CRDM replacement, so it is important so that a drop load scenario is avoided. I have now assessed Westinghouse's UK specific documentation (Ref. 35) which I found to be aligned to my expectations in respect of CRDMs.

4.7.2 Findings

AF-AP1000-ME-11: *I consider it to be an Assessment Finding that a future licensee shall carry out an inspection of the shims during the NPP operational life. In clarification, my expectation is that visual inspection of a CRDM shim should be carried out following the replacement of a latch assembly, without the need for a routine scheduled maintenance inspection requirement. Target Milestone – during operational phase as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.8 Isolation Valves Providing Containment Safety Function

179 During my Step 4 assessment, I further targeted the topic of isolation valves providing a containment safety function, selecting the motor operated valves that are associated with the Automatic Depressurisation System (ADS) due to their considered safety significance. I have reviewed the safety functions associated with these valves during my assessment, and the specific designs for their intended duty, to ensure that they are of a sound engineering principle, and have benefitted from appropriate Operational Experience Feedback. In addition, I decided to assess the arrangement to control and manage the spurious actuation of the Passive Residual Heat Removal Heat Exchanger (PRHR HX) isolation valves, which are considered to be of particular importance to safety.

180 I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle ECS.1 (Ref. 4) states 'The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety'.
- Safety Assessment Principle ESS.1 (Ref. 4) states 'All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.'

In particular the PRHR HX acts as a safety system to manage a number of fault scenarios by the provision of a heat sink.

181 In undertaking my assessment, I have also used the internal ND technical assessment guide, Design Safety Assurance, T/AST/057 (Ref. 7), to guide my process and conclusions.

4.8.1 Assessment

4.8.1.1 ADS System Valves

182 Westinghouse has provided information that explains that the ADS (Figure 2) acts in conjunction with the Passive Core Cooling System, whose purpose is to mitigate the consequences of a Loss of Coolant Accident. The system configuration consists of two

process trains, with each train branching off into 3 parallel lines, with each line containing 2 isolation valves in series. The first valve is a gate valve, which acts as reactor coolant pressure boundary isolation. The second is a globe valve which provides a second backup isolation role. A further process line containing a solenoid valve is provided. This line enables the gate valves to be tested during outages. It was noted that this valve also forms part of the reactor coolant pressure boundary, and so acts as a primary circuit isolation valve. The ADS also uses squib valves, which are discussed in more detail in Section 4.10 of this report.

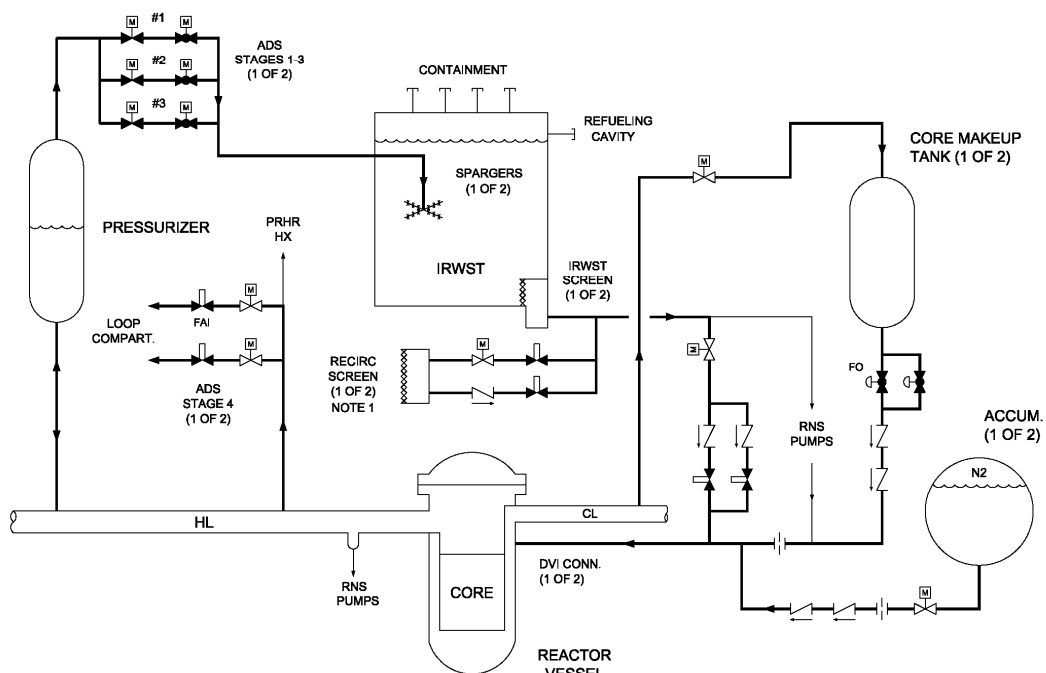


Figure 2

ADS Stages 1, 2 & 3 – Schematic Flow Diagram

- 183 Discussions identified the function of the solenoid valve and process line is to support the stroke testing of the gate valves. The branch allows the system either side of the gate valve to achieve equal pressure, which during EMIT stroking of the valve minimises valve degradation and wear, (which leads to valve leakage), so increasing the valve's operational life.
- 184 Westinghouse explained that a temperature leak detection system is fitted to each of the process branches downstream of the second isolation valve. Westinghouse's arguments for not having leak detection upstream of each globe valve are:
- Leakage past the first valve does not impact plant operations.
 - The first isolation valve is of a first design choice (Ref. 28).

- 185 Discussions confirmed that the valve selection followed the Westinghouse design process i.e. Electric Research Power Institute (EPRI) NP-6516 'Guide for application and use of valves in Power Plant systems' (Ref. 52), GW-P1-020 'Valve standardisation selection Criteria' (Ref. 53), and the ALWR Utility Requirements document.
- 186 Operating experience has led to the evolution of the gate valve design to be a uni-directional flex wedge gate design, which provides good leak resistance characteristics. To prevent pressure locking the upstream valve bonnet contains an aperture, which allows fluid into the wedge void, which in turn allows fluid either side of the sealing face to be of equal pressure. The flex wedge disk design also minimises the effect of thermal binding. However, I noted from discussion that during valve re-assembly under maintenance, the orientation of the flex gate is wholly reliant on personnel following the maintenance instruction. I consider this to be acceptable in principle, since EMIT associated with mechanical equipment does rely on the use of Suitably Qualified and Experienced Person (SQEP) personnel, although poka yoke features can be beneficial in this aspect.
- 187 On the loss of power each valve is able to be actuated from a separate battery supply, and the batteries are located in different battery rooms.
- 188 One of the safety requirements within the fault analysis is that each globe valve is required to open within the following time ranges:
- ADS Stage 1 - minimum opening time 20s and maximum opening time 40s.
 - ADS Stage 2 - minimum opening time 60s and maximum opening time 100s.
 - ADS Stage 3 - minimum opening time 60s and maximum opening time 100s.
- 189 As part of my assessment I confirmed that the valve technical specification captured the above requirements, and that the supplier designs within these limits and does not include for any additional margins. However, Westinghouse confirmed the above parameters encompass the appropriate margins from evaluating the design basis criteria and the accident analysis.
- 190 Westinghouse explained that Teflon material is not utilised within the valve design due to the degradation effects from the containment environment.
- 191 The selection of a globe valve type for the second redundant isolation valve is against the system operational criteria and for diversity reasons, which I consider to be a reasonable explanation.
- 192 The valve Equipment Qualification is detailed within AP1000 design documentation, which was provided by Westinghouse during my assessment process (Ref. 29, and 31). I considered it to be evident from discussion that the Westinghouse design philosophy of mechanical items is for their existing United States (US) customer base, with design substantiation being inline with the United States Nuclear Regulatory Commission (US NRC) Regulatory requirements. Westinghouse stated that the NRC has developed and issued various updates of their requirements, which take into account extensive operating experience. From this understanding I have a level of confidence in the quality and depth of equipment qualification associated with the AP1000 design. One observation however is that the AP1000 design is against a particular issue of standards, which may be subject of an update prior to the construction of a NPP in the UK. This aspect has been assessed in Step 4 and is reported under the Codes and Standards topic.
- 193 My sample assessment of a valve data sheet (Ref. 76) identified a number of safety functional requirements. An important aspect of the GDA from a Mechanical Engineering

point of view is assessing evidence of transferring the design intent through the project life cycle, i.e. from the initial identification of the safety functions at the conceptual stage, through the supply chain, and to the operational phase. I have sample reviewed several valve and pump data sheets, design specifications, during Step 4, which has provided me with adequate evidence of safety functional requirements being stated at this level.

194 Through progressing a Step 3 finding associated with the classification of PXS V129 A/B, which acts as reactor coolant pressure boundary isolation valves following actuation of the passive core cooling system, Westinghouse provided the evidence during Step 4 of a design change that was approved for implementation (Ref. 32). This changes the valve classification associated with PXS V129A/B, to one being in-line with my expectations. i.e. the test and drain line components are now assigned with an equipment Classification 1 due to the components in question forming part of the reactor coolant system pressure boundary. On assessing the evidence, I am now satisfied to close out this line of enquiry as part of the GDA.

195 During the procurement phase of mechanical items, Westinghouse generally utilises design specifications to transfer the design intent to a supplier, who typically becomes responsible for developing the concept through detailed design and into a manufactured item. The supplier is then responsible for functionally testing the item at the factory, in readiness for installation into the plant, while Westinghouse acts as a Responsible Designer throughout the process, and is responsible for accepting the detailed design and design substantiation. This topic is further discussed under the Squib Valves topic (relative to this equipment).

196 My assessment has identified that to date there are a limited number of mechanical items that have been assigned to a specific supplier and are complete in terms of detailed designed. As a consequence the ability to seek evidence from detailed design substantiation, and from carrying out the FATs has been limited. This has already been captured an Assessment Finding (**AF-AP1000-ME-02**) within this report.

197 In summary, I am satisfied with the information and explanations provided by Westinghouse covering the ADS motorised operated valves arrangement, and have not identified any areas of concerns from a GDA and Mechanical Engineering perspective against SAPs ECS1 and ESS.1.

4.8.1.2 PRHR HX Isolation Valves

198 A spurious actuation of the PRHR HX isolation valves would cause the injection of a relatively cold leg of water (10° C) into the Reactor Coolant System, which would lead to a reactivity increase due to increased moderation effects, which results in a rapid reactor power increase.

199 Westinghouse explained the scenario of this spurious actuation of the PRHR HX isolation valves. In these circumstances:

- No existing reactor trip can be credited.
- The fault results in a new equilibrium operating condition at a higher power level.
- The primary acceptance criteria are challenged.

200 Westinghouse's review of the analysis conducted to date also identified the inclusion of three non conservative assumptions:

- Boron concentration in the PRHR HX is at RCS level or higher.

- PRHR heat exchanger flow mixes perfectly in the steam generator outlet plenum, which evenly distributes the coolant between the two cold legs.
 - The current core inlet mixing model is based on hand calculations.
- 201 US licensing criteria limit the fuel centreline melt heat limit to 75kW/m; initial analysis (with potential non conservative assumptions) provided results of 73.7kW/m.
- 202 Through discussion Westinghouse explained that:
- It is not possible to confirm the even distribution of PRHR flow between the Reactor Coolant Pump (RCPs). Computational Fluid Dynamics analysis indicates an uneven split between the RCPs.
 - There is no process to control the PRHR heat exchanger boron concentration.
 - There is uncertain mixing within the reactor lower plenum.
 - Updated results determined a heat flux of 86.7 kW/m which exceeds the limit.
- 203 The above analysis output triggered the implementation of a design change (Ref. 36), which ensures the reactor trips on a spurious actuation of any of the PRHR isolation valves, within a timeframe that prevents a significant reactor power surge.
- 204 The revised design is to include:
- A reactor trip if the inlet valve is open and either of the outlet valves are open.
 - Four independent positional sensors on each outlet valve.
 - A reactor trip response time of less than 1.25 seconds.
- 205 Analysis incorporating the design change confirms there is no significant increase in power prior to a reactor trip. Power increase is limited to 0.8%, Departure from Nucleate Boiling (DNB) does not occur, and the fuel temperature limits are not challenged.
- 206 In summary, I am satisfied with the explanation that Westinghouse provided on this subject from a Mechanical Engineering perspective against SAPs ECS.1 and ESS.1, and my assessment of the supporting documentation (Ref. 36, Ref. 37) confirmed the design change is implemented within the GDA design reference. However, I consider it to be an Assessment Finding (**AF-AP1000-ME-12**) that all necessary AP1000 design and safety documentation is updated accordingly.

4.8.2 Findings

AF-AP1000-ME-12: *The licensee shall ensure that the design change associated with spurious operation of the PRHR HX has been completed to ensure that the reactor is tripped as necessary, and that all necessary AP1000 design and safety documentation has been updated accordingly. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.9 Check Valves

207 My assessment has identified that the design contains several check valves that are important to safety. I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment Principle ECS.1 (Ref. 4) states 'The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety'.
- Safety Assessment Principle EAD.1 (Ref. 4) states 'The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage'.

208 The AP1000 design incorporates various designs of check valves, with their selection being principally dependant on their safety and operational requirements. Types of check valve designs within the AP1000 plant design include:

- Swing check valves.
- Lift check valves for 2 inch or less applications.
- In-line check valves for the core make up discharge lines.
- Stop check valves.

209 As a consequence my Step 4 assessment has targeted their design and consideration in relation to:

- Safety categorisation and classification.
- Equipment qualification.
- Surveillance and EMIT.
- Operational experience.

210 In response to questions, Westinghouse confirmed that the AP1000 does not contain any tilting disc check valves; principally on the grounds that this design type inherently has a higher pressure drop across the valve than a swing check valve type.

4.9.1 Assessment

4.9.1.1 In-Line Check Valve

211 Of particular interest is the proposed in-line check valve for the core make-up discharge lines, which Westinghouse considers is a 'First Of A Kind' (FOAK) design within an NPP. Westinghouse confirmed that US plants have in the order of 20 years operating experience of 'similar' (but not the same) valves, where they are typically installed in the steam supply lines, and the valve is required to close on a line break. The difference for the AP1000 proposal is that the valve seat is normally open under no flow conditions, and the seat is only closed on an increased back flow pressure. The valve achieves its design intent by the valve seat being held in the open position via a spring.

212 My assessment has identified that the in-line check valve has a design life of sixty years, and is the subject of a development and equipment qualification programme, (Ref. 22). Westinghouse has also provided documentation which details the valve test specification. The test's purpose is to demonstrate the valve functionality, taking into account flow capacity and the effects of aging on the spring.

-
- 213 In response to questions, Westinghouse stated check valves that support safety functions are qualified in accordance with ASME. The associated quality level is commensurate with the check valve duty. i.e. Quality Group A (ASME Class-1) valves that form part of the RCS pressure boundary; Quality Group B (ASME Class-2) valves that perform a containment barrier function, fission product barrier, core cooling etc; Quality Group C (ASME Class-3) valves that provide support following a Design Basis Accident, e.g. safety injection, core containment cooling, negative reactivity provision etc.
- 214 Westinghouse confirmed that two in-line check valves, positioned in series, are included within the process design to manage the fact that operational experience provides evidence that check valve seats cannot be guaranteed to provide an isolation function.
- 215 The process pipework design typically incorporates test loops that allow safety check valves to be functionally tested during outages. The loop test allows:
- The valve position to be verified.
 - Confirmation the valve leak rate is within design limits.
 - The disc is stable in the open position.
- 216 I noted that the acceptance criteria for the testing is quoted within ASME, and will be stated within the Operating Technical Specifications.
- 217 Westinghouse advised that extensive operating experience is available on the subject of check valves and is captured within the AP1000 design e.g. SOER 86-03 captures check valve failures in industry. The US NRC issued guidance on testing of check valves both for open / closed positions and leak rates, which considered operational experience. The ASME OM Code, Appendix II (96) was updated to take into account operational experience and the US utilities have formed a Nuclear Industry Check Valve User Group which considers operational experience. The Westinghouse response to TQ AP1000-909 (Ref. 10) also covers operating experience for this type of valve for nuclear applications that provide a level of confidence on the reliability of the valve.
- 218 Discussions with Westinghouse identified that the valve is butt welded within the process line. Westinghouse explained that space constraints are driving this choice of fixing compared to utilisation of a valve fitted with flanges. As a consequence maintenance can only be carried out by cutting the valve from the line.
- 219 Westinghouse described the valve set up within the process line (Figure 3), and the justification for having the valve normally open on 'no flow and forward flow' and closing on 'reverse flow'. The type of valve in question is located downstream of each Core Make-up Tank and supports the Passive Core Cooling System. Each CMT process line contains two in-line check valves that are positioned in series. Located upstream are two globe valves that are positioned in parallel. During normal operations the upstream valves provide the passive core cooling isolation as they are normally closed. The inline check valves have no duty during this aspect of the process but are in the open position. On actuation of the ADS stages 1, 2 and 3 and the parallel isolation valves the Core Make-up Tanks passively inject boronated coolant into the reactor coolant system via the 2 open in-line check valves. The Probabilistic Risk Analysis (PRA) drives for the valves to be of a design that is set open with no flow so there is no consideration of an active failure to open on demand. On lowering the coolant level within the Core Makeup Tanks and the associated system pressure, the accumulators actuate under Nitrogen pressure to inject further boronated coolant into the reactor coolant system. During this injection process the two in-line check valves are required to close and isolate the line to the Core Makeup Tanks. Two in-line valves are incorporated to address the single failure criteria (i.e. one

valve suffering an active failure of 'failing to close'). I noted that the valves do not give consideration to passive single criteria failure whilst in their open position, and have identified this feature to my Fault Studies assessment colleagues. I understand this has been progressed via their RO in this area, Diversity of Frequent Faults and Consideration of Passive Failures, RO-AP1000-047 (Ref. 11).

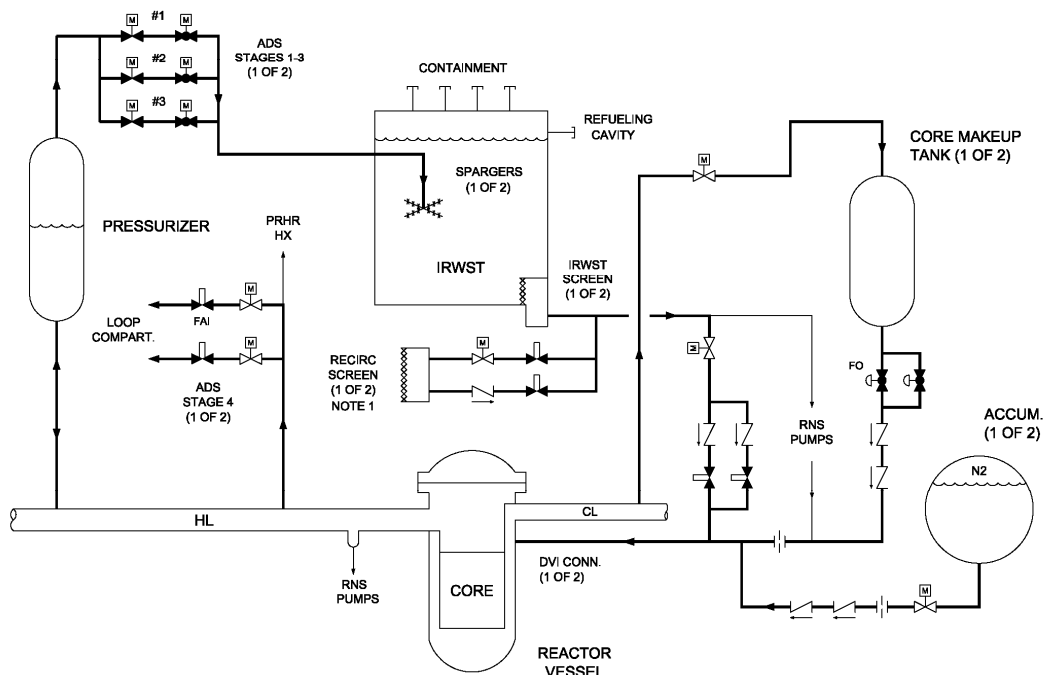


Figure 3

Passive Safety Injection - Schematic Flow Diagram

- 220 Westinghouse explained the valve characteristics of a low reverse flow of coolant being required to close the valve, and only a low pressure difference required to reopen the valve, as being important characteristics which have driven the selection of this valve design for the application.
- 221 One advantage of this type of valve is that it is of a compact design, has a short travel distance for the moving part, and has a very fast closing time. To offset against these advantages the valve has a relatively high pressure drop, and the entire assembly requires to be removed for maintenance.
- 222 Westinghouse advised that the recent Equipment Qualification type test had been successfully undertaken on the latest design of valve, which is now considered as the final design with the associated final design report (Ref. 23). In response to questions,

Westinghouse stated that the nominated supplier would undertake additional tests themselves, but this was a commercial decision to ensure that the valve would successfully meet the production test requirements. No further prototype tests are planned by Westinghouse.

223 My assessment has identified that a key feature of the finalised design is the provision of two ports within the valve body to facilitate in situ inspection and testing. One port is provided for visual inspection, and the other port facilitates stroking of the valve by water injection. These ports are blanked by sealing caps which have now been agreed through the DCP process as ASME Class 1 boundary closures. Pipe connections with valves are also provided to facilitate testing of each individual check valve (Ref. 24).

224 Westinghouse stated that no Final Design Review is planned for these valves, (explaining that such a review is only planned for the squib valves due to their novelty). However, they stated that a final design review is planned for the whole Passive Core Cooling System design. The Westinghouse response to TQ-AP1000-689 (Ref. 10) sets out the arguments in support of this strategy, which on balance I consider to be acceptable.

225 The aims of the recently completed prototype qualification test (Ref. 23) were:

- To determine the minimum flow rate required to close the valve and maintain closure.
- Verify the valve opens with no flow once the pressure difference is relieved.

226 The results confirmed the valve:

- Closes with a flow rate to specification, providing a margin of 27%.
- Opens on the accumulator pressure lowering to specification, providing a margin of 40%.

227 Discussion also highlighted that further qualification tests are planned with the first production valve. This is due to the prototype valve body containing a polycarbonate section to aid viewing of the internal parts during the prototype tests.

228 Westinghouse stated that on a production batch of eight valves, one valve shall be selected at random and be functionally and leak tested. Following the test the valve will be subsequently released for site installation into the NPP.

229 I consider from discussion that the valve functional performance has also been underpinned by carrying out a Computational Fluid Dynamics analysis.

230 My assessment of supporting documentation (Ref. 23 and 25) has confirmed:

- The design parameters for the valve are adequately captured. In particular the requirement for the valve to re-open after the accumulators have been actuated and the system pressure has adequately reduced allowing the Core Make-up Tank to drain to a level that signals the actuation of the 4th Stage ADS.
- Performance requirements are specified.
- Valve disk cycles (6000) are specified.
- Seat leakage class 4 (2cc/hr per inch NPS) is specified.
- Seismic Category 1 by computational analysis is specified.
- Testing requirements are specified.

231 In response to questions, Westinghouse confirmed the documents have been issued to the supplier.

- 232 My assessment has confirmed that positional indication is only fitted to a check valve if the individual valve supports a post accident monitoring scenario. The Westinghouse response to TQ-AP1000-685 (Ref. 10) response identifies check valves within the AP1000 NPP design that incorporate positional indication.
- 233 In response to questioning associated with the claim that the valve is of a “passive” (i.e. fail-safe in this context) design, (i.e. the valve disk is open on no flow, which is the normal operating condition), Westinghouse stated that the valve arrangement allows the Core Make-up Tank to discharge without the valve requiring to change position, which is accepted as being “passive” (i.e. fail-safe in this context). It was confirmed that the valve closes on the actuation of the accumulators to ensure the correct fluid flow into the main primary reactor coolant circuit. It was also confirmed that each in-line check valve is then required to open to enable the Core Make-up Tank to drain further to a level that actuates the 4th stage ADS, which is the trigger for the passive core cooling system. I now consider this process sequence, which requires the valve to close then re-open, classifies the valve as an “active” design (i.e. non fail-safe), and I have advised my Fault Studies colleague accordingly.
- 234 In response to questioning that the valve disk will be the subject of oscillation from the actuation of the accumulators, (following internal discussion with Fault Studies colleagues), Westinghouse claimed:
- The spring is of a design that the stresses are sufficiently low to provide an expected life into the millions of cycles.
 - The disc is a high strength-low mass design that is guided along its rod length by a nominal clearance.
 - The diffuser is of a vane and contour design to provide a degree of flow straightening.
 - The valve is to be qualified to ASME-QME-1.
 - Testing of similar valve designs has not identified issues.
 - Seismic analysis shows the valve will sustain a postulated seismic event.
 - Operating experience has not identified challenges with unsteady, turbulent, or oscillating flow unless the valve inlet is positioned in the close proximity of an elbow, (in which case difficulties appear to be limited to valves >16 inch nominal diameter with a toroidal disc configuration).
- 235 The valves are to be tested during each planned outage for disk closure, disk passing, and reopening on no flow. Testing is achieved via the system design incorporating a dedicated pipework arrangement, which forms part of the primary reactor coolant circuit and is isolated appropriately via an isolation valve and welded plug. This arrangement is being introduced into the design via a design change (Ref. 24), which is currently progressing through the Westinghouse design change process. My assessment has progressed assuming the inclusion of this design change. I consider the design change status to be an Assessment Finding (**AF-AP1000-ME-13**); the design change is to be implemented into the AP1000 NPP design, and all necessary design and safety documentation.
- 236 I also noted the valve design incorporates a test port. The purpose of the port is to allow a mechanical dip stick to be deployed during EMIT to verify and confirm the valve disk is in the correct position. The valve test port forms part of the primary reactor coolant system and thus is isolated by a piping arrangement that incorporates an isolation valve and a welded plug, which is in line with my expectation.
-

-
- 237 The system design eliminates the loss of excessive coolant during EMIT with the aid of dedicated EMIT isolation valves. The Westinghouse response to TQ-AP1000-678 (Ref. 10) describes the arrangements.
- 238 On reviewing the 3D model, I noted the EMIT valves and plugs are positioned at a height that will aid the testing activities. On this basis I judge that adequate access and working areas are provided to carry out the associated testing of each valve.
- 239 The valve is an integral part of the reactor primary coolant circuit, and maintenance of the internal aspects of the valve can only be carried out by cutting the valve out of its associated pipework since the valve is welded in place.
- 240 The in-line check valve was introduced into the design via a design change (Ref. 26) that improves the PSA claim to that associated with a valve that is normally open on no flow. The previous design incorporated a swing check valve, which was also a butt welded type, which I consider is the first design choice for fittings within the primary reactor coolant system. This standard swing check valve design incorporates a flange bonnet, which provides access to the valve internals components for inspection and maintenance when required. Nevertheless Westinghouse has explained the reasoning for selecting an in-line check valve for this application.
- 241 In response to questions, Westinghouse has stated that spatial constraints stopped flange type in-line check valves from being incorporated into the pipework design. The prime issue was insufficient space between the surrounding steelwork and the location of the pipework.
- 242 It is evident that spatial aspects are challenging at times within the AP1000. I consider this is principally due to the AP1000 design evolving out of the AP600 design, and whilst plant and equipment has been re-sized, the building footprint has not increased proportionately. I consider this aspect to be generic throughout the nuclear island design and as the design matures through its project life cycle and through operations it will inevitably lead to increased complexities with the system design, plant modification, and maintenance activities, which is likely to have associated personnel dose rate consequences. Although I recognise this is an intrinsic characteristic of the AP1000 NPP, I have raised a GDA Issue (**GI-AP1000-ME-03**) covering pipework EMIT activities which relates to this aspect (described earlier in Section 4.3 of this report).
- 243 Westinghouse claimed that the valve disk and internals are of an adequate design for 60 years, based on the valve design and qualification process for the specified 6000 cycles, whilst the valve internals are only called upon to operate in an accident scenario. I also consider it feasible to replace a valve by cutting it out of the pipework, and replacing it with a new valve, (although not ideal).
- 244 In addition, I judge the layout offers the provision to cut out a section of pipework, so if a valve is required to be replaced more than once, it is possible to avoid the cutting of the pipework and welding in an identical position; thus limiting any detrimental characteristic changes to the local pipework material due to the welding process.
- 245 Westinghouse has estimated the dose rate associated with this type of valve replacement is 0.7 rem/hr (7 milli Sv per hour). My subsequent discussion with the Radiation Protection assessment discipline has confirmed that this activity can be managed by necessary arrangements to limit personnel dose. I also judge that several aspects of the replacement tasks may be required to be carried out by remote means.
- 246 In summary in respect of the GDA and from a Mechanical Engineering perspective against SAPs ECS.1 and EAD.1, I consider the principle of the system design incorporating these in-line check valves is acceptable. This is based on the evidence
-

provided that the valve is being subjected to a robust qualification process; the valve is to be the subject of EMIT during each outage; the valve is closed via the actuation of the accumulators prior to the requirement for the valve to re-open to allow further drainage of the Core Makeup Tank; and there is provision to replace the valve if necessary.

4.9.1.2 Stop Check Valves

- 247 Following receipt of the Westinghouse response to TQ-AP1000-0747 (Ref.10) on the subject of stop check valves, I targeted my assessment on the Westinghouse justification for their selection for use within the AP1000 NPP design.
- 248 Westinghouse has described a stop check valve as a valve which in its open position acts in a similar manner to a check valve, therefore allowing flow in one direction only. However, the valve design also allows the valve seat to be set closed (by external action), which stops flow in both directions, therefore allowing the valve to act as an isolation valve. During a technical meeting Westinghouse tabled a drawing (Ref. 27) to illustrate both aspects of the valve functionality.
- 249 Westinghouse confirmed that the AP1000 plant design incorporates this type of valve in 3 locations, which are:
- APP-RNS-PL-V015 A.
 - APP-RNS-PL-V015 B.
 - APP-CVC-PL-V081.
- 250 The Westinghouse Valve Selection Criteria (Ref. 28) identifies this type of valve as not being the first design choice. Westinghouse explained that the plant spatial constraints have driven the use of this type of valve in the stated locations. If spatial constraints were not an issue then the design arrangement would have proceeded using their first design choice of a stand-alone check valve for the direction flow control with a separate gate valve for the isolation aspect. Westinghouse explained that the APP-RNS-PL-V015 A/B valves are closed infrequently, for the unusual requirement to re-circulate the IRWST when the RCS pressure is low. Valve APP-CVC-PL-V081 is also normally operated as a check valve to support the purification loop return, which is operational for as much time as possible (essentially continuously). The valve is used in its isolation mode to divert return flow from the RCS loop to the pressuriser auxiliary spray line and the PXS equipment, and as such must close against only a modest differential pressure. Westinghouse considers the use of stop check valve an acceptable valve type for this type of isolation.
- 251 Discussion identified that valves V015 A/B are manually operated and the valves are not fitted with any locking devices to ensure they are correctly aligned with the process requirements; (this subject has been discussed previously under Good Engineering Practice). Valve V081 is air operated when being used as an isolation valve, and on loss of air it still retains its function of operating as a check valve.
- 252 I consider the use of stop check valves within the system design to be an Assessment Finding (**AF-AP1000-ME-14**); a future licensee to generate the ALARP arguments to justify each application of a stop check valve within the AP1000 NPP design.

4.9.2 Findings

AF-AP1000-ME-13: *The core make-up discharge lines in-line check valves are to be tested during each planned outage for disk closure, disk passing, and reopening on no flow. Testing is achieved via the system design incorporating a dedicated pipework arrangement, which forms part of the primary reactor coolant circuit and is isolated appropriately via an isolation valve and welded plug. This arrangement is being introduced into the design via a design change, which is currently progressing through the Westinghouse due process. The licensee shall ensure that this design change has been completed, and all necessary AP1000 design and safety documentation has been updated accordingly. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-14: *The licensee shall generate an ALARP argument to justify each application of stop check valve within the AP1000 NPP design. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.10 Squib Valves

253

During my Step 3 assessment, I raised a Regulatory Observation AP-1000-036 (Ref. 11) in respect of the squib valve concept and associated design substantiation. I had significant concern regarding the status of the design, its development, and the programme for future work. As a consequence I have targeted a sizeable proportion of my Step 4 assessment effort on the squib valve topic to progress the need for adequate arguments and evidence to satisfactorily close out the Regulatory Observation Actions. I consider the following Safety Assessment Principles to be relevant to this aspect of my assessment:

- Safety Assessment Principle ECS.5 (Ref. 4) states '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 item will perform its safety function(s) to a level commensurate with its classification.'
- Safety Assessment Principle ERL.1 (Ref. 4) states 'The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.'
- Safety Assessment Principle EMT.2 (Ref. 4) states 'Structures, systems and components important to safety should receive regular and systematic examination, inspection, maintenance and testing.'
- Safety Assessment Principle EQU.1 (Ref. 4) states 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'

254

In undertaking my assessment, I have also used the internal ND technical assessment guide, Design Safety Assurance, T/AST/057 (Ref. 7), to guide my process and conclusions.

255 As the squib valve design is an unusual and novel concept, and one that has not been utilised in previous NPP designs in such a role, the Multi Discipline Evaluation Programme (MDEP) has also shown interest in the topic (see Section 4.28). This has resulted in the generation of a common position on the design and use of squib valves in NPPs across the participating Regulators. In addition, and to be transparent and share knowledge and understanding of the squib valve designs with other Regulators, I invited the attendance of other Regulators (as observers) to a number of Step 4 technical meetings with Westinghouse.

4.10.1 Squib Valve Overview

256 A squib valve is a valve that provides zero leakage during normal operations. Actuation is via a pyrotechnic process, which is triggered by an electronic control signal. Valve actuation enables a rapid transfer of fluid and the depressurisation of the associated system pipework. Actuation of this type of valve is a once only sequence, unless the valve is refurbished. Mechanical valves can generally be stroked under EMIT regimes, which provides confidence in their reliability and associated safety function. This capability is not available for the squib valve designs. The inability to stroke the valves as part of the specified EMIT requirements was a significant consideration in guiding the depth and breadth of my assessment for this mechanical valve type.

257 The actuation process involves an electronic control signal firing a squib (small pyrotechnic charge), which in turn sets off a propellant charge. The propellant charge generates sufficient pressure to break the internal tension bolt. The generated kinetic energy then drives the piston which shears the valve shear cap, which results in the depressurisation of the system pipework and the transfer of fluid.

258 The AP1000 design incorporates 2 different valve design types in principle; an 8 inch type which is in line in a section of pipework, and a 14 inch type which is at the termination of a leg of pipework with its exhaust port open to containment.

259 The AP1000 14 inch squib valve is of a design that includes a single shear cap, which is positioned within a clamping arrangement that provides the necessary guidance to relocate the sheared cap in its post actuation position.

260 The AP1000 8 inch squib valve is of a design that includes two shear caps. The design of the piston entraps both shear caps and on valve actuation relocates the sheared caps in their post actuated position. Dependant on the system design application the 8 inch valve design can either be classed a "high" or "low" pressure valve. The difference in designation affects the detailed design of the cartridge, propellant load, tension bolt and shear cap, but not the valve principle of operation.

4.10.2 Assessment

4.10.2.1 System Description

261 The AP1000 Automatic Depressurisation System (ADS) design (Figure 4) consists of 4 Stages. The first 3 Stages consist of 2 trains, all fitted with motor operated valves. Stage 1 is 4 inch nominal size, Stages 2 and 3 are 8 inch. Stage 4 consists of 4 individual 14 inch squib valves, 2 attached to each of the hot legs on the Reactor Coolant System pipework. I consider the ADS system contains a level of component diversity by the system design incorporating various different valve types.

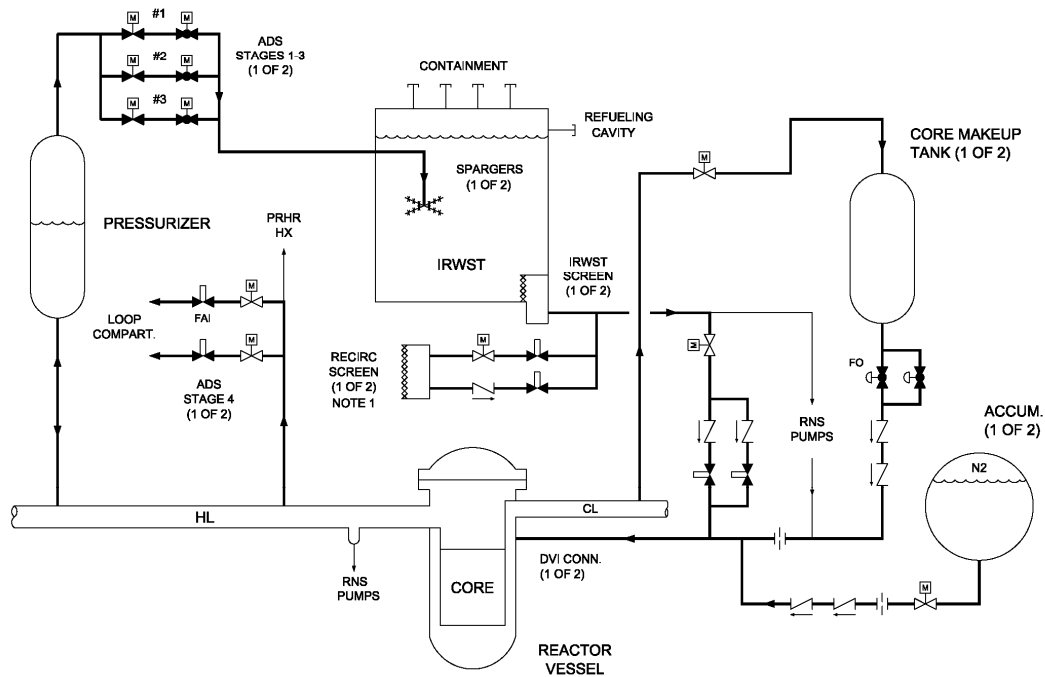


Figure 4

AP1000 Automatic Depressurisation System - Schematic Flow Diagram

262 In addition to the squib valves in the ADS, the design incorporates 8 inch squib valves which support:

- The Passive Core Cooling System by injecting boronated water from the IRWST into the Reactor Coolant System pipework, following the actuation of the 4th Stage ADS valves.
- The recirculation of boronated water from the containment sumps into the Reactor Coolant System pipework, to support the long term cooling of the reactor following an accident.

263 The injection system consists of two trains, with each train containing 2 off 8 inch squib valves that are positioned in parallel branches.

264 The recirculation system again consists of two trains, with each train containing 2 off 8 inch squib valves positioned in parallel branches. In this system each train contains one squib valve that contains shear caps that have a thinner shear section, which allows actuation with a lower force.

265 Westinghouse has confirmed that the only squib valves in the AP1000 design are those that support the 4th stage ADS and the Passive Core Cooling System.

4.10.2.2 Design Development Process

4.10.2.2.1 Process and Planning

266 I consider a fundamental aspect of evolving a new component design is that a Responsible Designer implements adequate arrangements to ensure a component is developed in a rational manner, generating arguments and evidence to justify the design is able to achieve its safety and functional design intent. This also requires that assumptions are sufficiently well understood so that uncertainties are either designed out or adequate measures incorporated to manage them.

267 A technical meeting was held in November 2009 to allow Westinghouse an opportunity to demonstrate they were undertaking the development of the squib valve designs to a formal, robust design process, with due consideration to the design constraints.

268 Discussion identified that Westinghouse's selection of the squib valve concept for the AP1000 design is based on considerations of reliability, plant diversity, and design simplicity. It is my expectation that the audit trail that underpins the valve selection is formally documented as it forms part of the AP1000 NPP design substantiation.

269 During discussion Westinghouse clarified the following points:

- They were developing an analytical model to evaluate the issue of excessive stress in the interconnecting process pipework on valve actuation.
- They were considering the impact of material aging on the stainless steel valve body casting when carrying out material degradation analysis.
- The equipment qualification tests are to take into account operating parameters such as aging, process temperatures, and pressure.
- Equipment qualification testing is now scheduled to be outside the GDA Step 4 timeframe.
- Equipment qualification is going to be based on the ASME QME -1 with additional regulatory guidance specified by the US NRC (as per existing motor operated valves).
- The design specification contained a design constraint that interchangeable valve components are 'Poka Yoke' (meaning they are designed to only fit if in the correct orientation and to a specific size of valve).
- Design substantiation is to be collated within suitable documentation.

270 My assessment to date considers the design is taking significant credit from the fact that a similar concept of squib valve design has previously been undertaken by General Electric.

271 I consider Westinghouse's description of their project plan (Ref. 42) provides adequate evidence that the project is set up and being carried out in accordance with Westinghouse's internal design process arrangements.

272 During my assessment I reviewed the detailed development programme supporting the squib valve designs to gain a level of confidence that the design was being adequately managed and controlled. My sample assessment of the programme identified 2062 scheduled activities with a start date of 6/9/07, which continued through to 21/7/10. In response to questions on the detail of the programme, Westinghouse identified the

programme activity that reviewed the FMEA to verify that the updated design constraints have been satisfactorily incorporated. They also demonstrated the sequence of a design process for the revised tension bolt design, which included: an initial design activity, a design review, and a detailed design activity. The above sample assessment provided a satisfactory level of evidence that the evolving squib valve designs were being managed and controlled under a formal design process.

273 Westinghouse confirmed the FMEA was scheduled to be reviewed and updated to reflect the latest design. This aspect is part of the GDA Issue (**GI-AP1000-ME-01**); it is my expectation that such a review to be undertaken by SQEPs, and with some independent technical input to review the final proposed designs. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.10.2.2.2 Design Review

274 My assessment has now confirmed that a technical design update review has been undertaken, which focused on the closure of the [REDACTED] action items that had previously been raised at the Intermediate Design Review.

275 In July 2010 I attended the squib valve Final Design Review (FDR) as an observer to gain a further appreciation of Westinghouse design process.

276 I consider the basic purpose of a design review is to ensure that the design intent, interfaces between disciplines, optimisation of the design, and essential health and safety requirements are being achieved. I consider that multi-discipline design reviews are primarily undertaken to review the design from a holistic aspect and to confirm that interfaces between disciplines are adequately considered; whereas single discipline design reviews are primarily undertaken to permit the input from functional expertise to assist in the optimisation of a design.

277 A design review is a structured process, which uses the experience and judgement of peers and senior engineers to independently review and confirm the adequacy of a design.

278 [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

279 [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

280 The review summarised the prototype testing, by stating that all [REDACTED] tests carried out achieved their full flow objectives verifying the Computational Fluid Dynamics analysis. The valve bodies did not incur any damage during the tests and the design reports (Ref. 70), which include a further overview of the sensitivity analysis, are approved.

281 I made the following observations from attendance at the meeting, which I discuss in detail later within this report:

- The review did not cover maintainability aspects of the valves or associated systems.
- That neither valve design incorporates a feature that provides an indication that the valve piston is correctly positioned during normal operations, so that the operator knows it is available to actuate on demand.
- The 14 inch squib valve exhaust port is still of a design that is open to containment, and at risk of collecting debris and items that could impair the valve performance.
- The revised 14 inch squib valve positional switch design is potentially fragile and susceptible to damage, impacting its operability.
- There was no discussion on surveillance and EMIT requirements or plant spatial aspects.
- The ADS 7 – 14 inch valve test incorporated all the current design changes to date.
- The only outstanding testing of the squib valves are now the equipment qualification tests.

282 In summary, I consider that the design review demonstrated that the development had taken into account information from tests undertaken to date, as well as the increased understanding of the design parameters which affect the squib valve performance and design. Nevertheless, it also confirmed my previous judgement that at the start of Step 4 the squib valve designs were at a relatively early stage of design development.

4.10.2.2.3 Maintainability Studies

- 283 To progress my observations from attendance of the FDR, Westinghouse has described their maintainability studies, which were initiated during the summer of 2010 and are being undertaken for the whole of the AP1000 design. The studies aim to provide the utility customer with the ability to maintain the AP1000 in a safe, time efficient, and cost conscious manner.
- 284 The studies have adopted a multi-faceted and diverse approach, comprising COMIT workshops (Constructability, Operability, Maintainability, Testability), and layout maintainability team walk-throughs. The maintainability team includes input from the layout design team, NPP Operations and Maintenance personnel, NSSS and Balance of Plant (BOP) installation / removal support, and human factors support for risk significant components. The detailed process commences with a job pre-brief, then moves to reviewing the COMIT and seismic outputs, to producing a Situation Overview Paper, which is then subjected to a maintainability peer review. The process has the potential to lead to additional DCPs in order to achieve the maintainability requirements.
- 285 Westinghouse has not yet looked at UK specific legislation in terms of Health and Safety associated with maintenance activities. Furthermore the design for decommissioning is not explicitly covered as part of this process, although this is looked at via separate studies. It is my expectation that both of these aspects need to be incorporated into their process for a UK plant. It is worth noting that UK legislation in this area is generally not prescriptive, and is subject of the general ALARP approach since it was derived from the Health and Safety at Work Act. However, I am satisfied that this area can be taken forwards as normal regulatory business into Phase 2.

4.10.2.2.4 Responsible Designer Role

- 286 As part of my assessment of the squib valve design and its development process, I decided to further challenge and assess Westinghouse's design role in the process, since much detailed design and development is being undertaken by their suppliers for this equipment.
- 287 In response to TQ-AP1000-0852 (Ref. 10) Westinghouse described how they act and retain the role of Responsible Designer: from the initial valve selection, to specifying the valve and system constraints, to supervising and managing the design, to design acceptance as the valve design finalises, and through to valve procurement.
- 288 During discussions Westinghouse has confirmed that they evaluated and were responsible for selecting the squib valve concept, and leading the design development, with support from specialist suppliers and consultants.
- 289 My assessment of the Technical Specifications has provided evidence of Westinghouse acting as a Responsible Designer in defining the safety requirements, design considerations and the acceptance of the detailed design and its substantiation, (Refs. 42, 45, 57 & 65).
- 290 Westinghouse has conducted several design reviews as the valve designs have evolved following their WEC 3.3.1 procedure (Ref. 58). Due to the valve's novel design Westinghouse has also sought numerous internal and external experts to aid the valve development process.
- 291 Through my assessment, I have gained a degree of confidence that Westinghouse has developed an adequate Responsible Designer role from a Mechanical Engineering and a GDA perspective in developing the squib valve design.

4.10.2.2.5 Design Development Summary

292 In summary, and at the end of GDA, I now consider my assessment has provided a reasonable level of confidence that the squib valve is generally following a rational and structured design process.

4.10.2.3 Prototype Testing and Design

4.10.2.3.1 Tests Reported

293 During the Step 4 timescale Westinghouse has carried out a number of prototype tests in support of understanding and substantiating the squib valve development and designs, which are documented within the appropriate test report (Ref. 70). One test in particular (Test – ADS 6) for a 4th Stage ADS 14 inch squib valve was witnessed by the European Utilities, and other nuclear industry stakeholders. I did not attend the test, but I was later briefed by both NRC representatives and Westinghouse who had witnessed the test.

294 The test was performed inside a warehouse and at an ambient temperature. The setup was similar to previously performed tests but with the inclusion of an upstream pipeline that was filled with fresh water at supply temperature, and at a pressure that represented plant conditions following the actuation of ADS stages 1, 2 and 3.

295 On performing the test, the valve opened and the water discharged out of the valve exhaust in a cylindrical manner. After approximately 30 seconds the water stopped exhausting, smoke and water vapour was then observed coming from the valve open exhaust. This is considered to be associated with the pyrotechnic process and the firing of the cartridge propellant.

296 Westinghouse's inspection of the valve following actuation identified a bolt (each retainer has 2 bolts) had sheared from one of its guides (design has 2 retainers). This feature provides support to the shear cap and clamp during and following actuation.

297 Westinghouse has subsequently carried out an analysis of the failure, which is documented in a design calculation (Ref. 60), and which has resulted in the valve design being modified.

298 My assessment of the prototype test results has identified that out of 3 prototype actuation tests that represented the upper propellant parameters (120% loading), 2 tests (although the valve actuated) resulted in components failing to achieve their full design intent (i.e. without permanent deformation to non sacrificial parts). On review, I consider the Westinghouse calculation (Ref. 60) not to be a 'calculation' to my understanding of the term, but rather an engineering evaluation judgement. However, on balance, and noting that the squib valve qualification tests are scheduled to be undertaken in the future and a further identical test to Test ADS 6 is to be completed as part of the qualification test schedule, I can understand Westinghouse's reasoning for going forward. However, I consider the absence of carrying out Equipment Qualification tests (during GDA) to be part of the squib valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate adequate evidence that the squib valve Equipment Qualification tests demonstrate that each squib valve type is able to achieve its design intent.

4.10.2.3.2 Energy Absorbing Feature (8 inch squib valve)

299 The role of the crush tubes is to absorb the excess kinetic energy generated from the firing of the propellant and transferred into the valve's piston. The tubes limit the transfer

of loads into the valve body and supports, as the piston arrives at its end of travel stroke. The valve is designed to be fully open with a piston travelling the design value. Travel in excess of this design value results in the aperture within the piston restricting the flow path which may impact the valve flow capacity and characteristics. The tubes are of a design that limits the travel to this design criterion.

300 The response to TQ-AP1000-843 (Ref. 10) and associated discussion provide Westinghouse's arguments as to why the alignment margins associated with the 8 inch squib valve energy absorbing pipe feature are not eliminated by the design, i.e. by the size of the piston aperture.

301 Increasing the size of the aperture would result in the piston length increasing, which would have an impact on the valve body design, valve envelope, validation of the valve prototype test data, and system interfaces; hence one of Westinghouse's arguments for not having pursued this option.

302 The 5 prototype tests undertaken show no evidence that the piston travelled in excess of the design value limit. Plus the 120% propellant load tests (2-off) represented a bounding scenario for the applied energy to the piston, which is in excess of what will be seen within a production valve.

303 Westinghouse has undertaken:

- Analysis of static and dynamic tube crushing.
- Dynamic compression testing to understand the basic behaviour of the tubes and to eliminate diameter / length / wall thickness combinations that fractured or exhibited gross buckling failure modes.
- Static axial compression tests of tubing on a tensile test machine to quantify tube load and to attain acceptance criteria for batches of tube material, which is to be performed on the production lots.

304 In conclusion, I consider on balance that this design feature (which is also present in the 14 inch squib valve) has been the subject of an adequate design process, adequately analysed, and prototype tested for the current design to achieve its design intent.

4.10.2.3.3 Valve Position Indication

305 I noted from attending and observing the squib valve Final Design Review that neither valve design incorporates a feature that provides an indication that the valve piston is correctly positioned during normal operations so that the operator knows that it is available to actuate on demand.

306 My assessment has identified:

- That a finite element analysis has been carried out on the tension bolt design and a full scale shaker table test is to be performed as part of the valve's Equipment Qualification programme.
- The material procurement and manufacturing specification placed specific controls on the tension bolt design parameters, which also included a batch acceptance test.
- The surveillance and EMIT requirements identify the piston position is verified during refuelling outages. The 8 inch valve design is verified via deployment of a dip stick on removal of a cartridge, (although noting that only 20% of cartridges are removed during an outage). The design of the 14 inch squib valve has provision to verify the

piston position via its exhaust port i.e. without the requirement to remove the cartridge from the valve.

- The design change process has rejected a design change that proposed the incorporation of a feature that confirmed the piston position during normal operations. Westinghouse has advised that the design change was rejected at the peer review stage, and not by the design change review board so no formal minutes are available.

307 This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue an ALARP justification that each squib valve type as proposed is adequate to achieve its safety functional requirements and its design intent, in terms of position indication during normal operation.

308 The 14 inch squib valve shear cap final (actuated) positional indication switch design was revised following early results of the prototype tests and the increased system temperature constraint, when it was found that the shear cap damaged the switch on actuation. Westinghouse explained that the revised design was tested as part of the final prototype tests. The change involved developing the design so that the shear cap clamp, on actuation, does not directly impact the positional indicator switch and thus subject the switch to damage from the impact load.

309 My assessment considers the switch design proposal to be somewhat fragile and its position on the valve makes it susceptible to damage during plant operations. In response to questions, Westinghouse confirmed that a design change (Ref. 10; TQ-AP1000-1089) is being processed to incorporate a guard to protect the switch. The current proposed design is a bracket to support the instrument cable rather than a guard to provide protection for the valve position indicator. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue an ALARP statement on how the bracket design achieves the design intent of a guard.

4.10.2.3.4 Shear Cap

310 The design now incorporates bolts to position the 14 inch shear cap in place within the valve body to aid:

- Correct alignment of the shear cap with the shear clamp mechanism.
- Transportation requirements from the suppliers to installation on site.

I consider this design feature to be an appropriate solution to achieving these objectives.

311 Part of the EMIT is to carry out visual inspections of the shear caps for potential leaks. My assessment has determined that with the 14 inch ADS squib valve shear cap it is possible to carryout an inspection via the valve exhaust port.

312 Drawing D-402112 Rev 0 (Ref. 79) depicts the 8 inch squib valve design, which entraps both shear caps within the piston. It is unclear how a visual inspection of the shear caps can be carried out, with the current designed access plug that is located within the valve body. This is to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall provide the detailed evidence that an adequate visual inspection can be carried out on the 8 inch squib valve design.

313 TQ-AP1000-683 (Ref. 10) response provides Westinghouse's arguments and justification to their selection of Inconel 690 material for the shear caps, which I consider is reasonable and rational for such an application.

4.10.2.3.5 Valve Exhaust Port Cover

- 314 A 14 inch squib valve exhaust cover has not been designed at this time. However, I consider that the valve exhaust port has provision (a machined face and several blind tapped holes) which would allow the design of a suitable cover, to prevent debris from entering the exhaust port and detrimentally affecting its functionality.
- 315 At the December 2010 technical meeting Westinghouse stated that the 14 inch ADS valve design is to progress without a cover on the exhaust port, which was previously an open item within the design. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue an ALARP statement on how the 14 inch ADS squib valve design achieves its design intent without the requirement of a cover.

4.10.2.3.6 Poka Yoke Features

- 316 The response to TQ-AP1000-932 (Ref. 10) and discussions confirm the valve designs incorporate adequate poka yoke features to ensure subcomponents are fitted to the correct type of valve, which can be summarised as:
- Each tension bolt type has a different thread size, which ensures it is fitted to the correct piston and valve bonnet.
 - Each piston type therefore has a specific size tapped hole, which ensures the correct tension bolt is fitted.
 - Each valve bonnet type therefore has a specific size tapped hole, which ensures the correct tension bolt is fitted. In addition the cartridge well is different for all three cartridge types, which ensures the correct type of cartridge is fitted.
 - Each cartridge type has specific external parameters, (diameter and height) that ensure the correct fitting of a cartridge to a specific valve bonnet.
 - Each shear cap is positioned within the valve body by bolts, which are on a specific pitch circle diameter to suit the valve type. In addition the valve body has specific tapped holes to suit specific shear caps.
 - The 8 inch valve body contains an arrow to indicate flow direction on its external surface to ensure each valve is fitted into plant in the correct orientation.
- 317 I am generally satisfied with the assessment on the squib valve poka yoke design features. However, I consider the 8 inch squib valve design drawings sampled do not provide adequate evidence of the poka yoke features described in the technical discussions with Westinghouse. I therefore consider this aspect to form part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall provide confirmatory evidence of the described poka yoke features within the 8 inch valve detailed drawings.

4.10.2.3.7 Categorisation and Classification

- 318 The AP1000 Safety Categorisation and Classification report (Ref. 35) provides the evidence that the squib valves are assigned with a safety Categorisation of A and Classification 1 which is aligned with my expectations.

4.10.2.3.8 Prototype Testing and Design Conclusion

- 319 In conclusion and summary, whilst undertaking my Step 4 assessment, the squib valve designs have continued to evolve, which has resulted in limited availability of formally

documented arguments and evidence to support the squib valve final designs. This has been a significant contributory factor in resulting in the issue of the GDA Issue (**GI-AP1000-ME-01**).

4.10.2.4 System Considerations

4.10.2.4.1 Reliability Claim

320 Through discussions Westinghouse has described the squib valve reliability and diversity claims, and features. Diversity is identified as a requirement to counter the threat of Common Mode Failure in providing cooling to the core in the event of a LOCA. The diversity requirement is identified for the 8 inch squib valves, which leads the design for each of the two recirculation sumps to contain one Low Pressure (LP) valve type, and one High Pressure (HP) valve type.

321 Westinghouse claims a reliability of 5.8×10^{-4} (failure to open on demand) for squib valve operation; this figure compares to a pfd of 2×10^{-3} for an Air Operated Valve (AOV), and 4×10^{-3} for a Motor Operated Valve (MOV). The value of 5.8×10^{-4} is derived from the following three values:

- EPRI data (from Nuclear Regulatory Commission Regulations (NUREG)/CR-4550 for a MOV) pfd of 3×10^{-3} .
- [REDACTED]
- [REDACTED]

322

[REDACTED]

323 The reliability data is underpinned by the large experience base of over 100 000 squib valves built, and over 5 000 fired, (albeit smaller valves but operated in similar or harsher environments), without failure to operate on demand. Westinghouse has no information on inadvertent firing.

324 Westinghouse considers the reliability data for the smaller squib valves can be read across to the AP1000 design because the same design approaches and standards have been used; including engineering analysis, proof and leak testing, over and under loaded boosters during testing, and the same shearing material design concept.

325 Westinghouse claims the AP1000 design is not oversensitive to the squib value pfd, and indicatively if the pfd doubled, then the core damage frequency increases by circa 15%. I have discussed this with my PSA assessment colleagues, and the sensitivity result appears reasonable.

326 Westinghouse's claim of diversity between the LP and HP valves is based on a smaller cartridge, thinner tension bolt, and a thinner thickness shear cap. Westinghouse has considered other ways of achieving diversity, including use of a different manufacturer / vendor, which they have considered not practicable. Westinghouse considers the use of a different valve type defeats the benefits of the squib valve design concept / principle.

327 The TQ-AP1000-674 (Ref. 10) response identifies the sub components that may affect the actuation process reliability, their failure modes, and measures incorporated in the design to manage them.

328 I do not accept Westinghouse claim of full diversity in respect of the operation of these two 8 inch squib valves. I consider the LP and HP designs are different, however I do not

accept that they are diverse in the commonly understood use of the term. I have also provided my opinion on this matter to the PSA assessment team.

329 The Westinghouse response to TQ-AP1000-674 (Ref. 10) has subsequently advised that the PRA sensitivity study does not require to place a diversity claim on the HP and LP shear caps.

330 Based on the fact that the squib valves are a development item with no statistical information for directly equivalent designs being available, my assessment has targeted Westinghouse's design process to seek evidence that they have evaluated the critical parameters in an adequate and conservative manner. It is my expectation that the valve designs contain margins that are commensurate to their novelty and importance to safety.

331 Westinghouse has undertaken a sensitivity analysis (Ref. 70) of the squib valve designs, which has looked at each sub component that supports the actuation process and its sensitivity contribution to the design holistically. My assessment has confirmed:

- The analysis was undertaken by a team that consisted of SQEP personnel both within Westinghouse and from other appropriate external organisations.
- Each sub-component was analysed, to understand the material properties, manufacturing tolerances, the process sensitivity to the variables, and the influence of the variable on the functionality of the valve in achieving its safety function.
- The analysis data was utilised in defining the second round of prototype testing, to define the bounding design parameters.

332 My assessment has also identified that to manage and control the variables of the critical sub components a number of arrangements are required to be implemented during the procurement and manufacturing phase. Examples of arrangements include:

- Stringent control of material characteristics and processes to manufacture and test various components, example components include: the shear caps, tension bolts, and propellants.
- Lot testing of several components, examples include: shear caps, tension bolts, and cartridge propellants.
- 100% FATs inspection of several components.

333 I have assessed the analysis and I consider it to be generally aligned with my expectations. It provides evidence that Westinghouse has undertaken (as part of their design process) an analysis to understand the variables and sensitivity impacts of the critical components of the valve designs. However, stringent arrangements are required to be implemented during the valve procurement phase to support the reliability of a number of critical components, and at this stage there is limited evidence of these arrangements. I consider this to be an important part of Westinghouse's arguments to help compensate for the inability to stroke the valve under a proposed EMIT regime. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall provide evidence that adequate arrangements are in place to control and manage the supply of the squib valves, and tolerances for the technical parameters of critical components.

4.10.2.4.2 Interconnecting Pipework

334 My assessment of interconnecting system piping analysis has identified the activity is ongoing and remains an open item with packages being split into their various trains.

335 The piping analysis integrates the squib valve loads from two aspects:

- Hydrodynamic loads
 - i) From the 4th stage ADS, which are based on analysis and consider the depressurisation wave and steady state loads.
 - ii) From other squib valves, which consider the “near” instantaneous void that is created in the pipework from the sudden pressure differential during the actuation.
- Actuation loads, which are derived from prototype testing and consider the impulse loads acting vertically on the valve.

336 Piping analysis is being undertaken using the recorded prototype testing actuation energy loads, which has resulted in the introduction of a design change (Ref. 47). The design change increases the staggered time between the actuation of the first, and second squib valves to 60 seconds for each 4th stage ADS train. In addition the injection squib valves, which are actuated from a signal following the actuation of the 4th stage ADS valves, are to be staggered to reduce the system pipework loadings. On actuation of the injection squib valves the swing check valves provide the RCS pressure boundary isolation function (Figure 4) for a short duration until the RCS pressure decreases below the gravity head provided by the IRWST water.

337 The introduction of the recirculation squib valves and the aim of limiting the number of squib valve designs within the plant introduced a design change (Ref. 51) that revised the sizing of the RNS pipework. My assessment has confirmed that if one of the recirculation lines fails to open on the train that feeds the RNS, then the IRWST is able to provide the required flow of water through the other open train lines.

338 Westinghouse has provided evidence that the impact of the chemicals and pyrotechnic by-products transferring into the main injection process line following an actuation of an 8 inch squib valve has been evaluated, and was considered to be acceptable (Ref. 43). I have not assessed this in detail, but recognise that the squib valves operate in the event of a LOCA, and so I consider that any minor detrimental chemical effects are not significant in this context.

4.10.2.4.3 System Considerations Conclusion

339 In summary, I am generally satisfied that the Westinghouse design process has given adequate consideration to integrated system requirements from a Mechanical Engineering and a GDA perspective. However, stringent arrangements are required to be implemented during the valve procurement phase to support the reliability of a number of critical components, at this stage there is limited evidence of these arrangements. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**).

Pyrotechnics 4.10.2.5

4.10.2.5.1 Pyrotechnic Role and Duty

340 All AP1000 squib valves use the chemical energy contained in pyrotechnic boosters to provide sufficient energy to shear the shear caps. The boosters act as gas generators; the subsequent pressure gives kinetic energy to a piston which hits and cuts the shear cap.

341 Each squib valve includes a cartridge which is an assembly of a booster with two or three initiators (depending on type of valve), providing redundancy, to ignite the booster load. A cartridge is also called an actuator. These definitions are provided by the Pyrotechnic

Actuator Requirements (Ref. 65). The pyrotechnic substance used for initiators is different than that of the main load (booster). The propellants selected for initiators and for boosters are respectively called P1 and P2 in the following sections.

342 Each initiator is electrically fired by dedicated ignition lines, connected to an electronic device. Within the Protection and Safety Monitoring System (PMS), this device is called a termination unit; within the Diverse Actuation System (DAS), it is called a terminal block. Upstream, all termination units are commanded from the Control and Instrumentation (C&I) of the Nuclear Power Plant. Terminal blocks are manually commanded. Termination units and terminal blocks are designated further as an Electronic Ignition Circuit (EIC) in this report.

343 The C&I assessment of this system is covered in another dedicated technical report.

344 In order to comply with UK Law, the squib valves' design shall give due recognition to ALARP principles. Notably, the pyrotechnic concept, the propellants selected and the type of ignition shall entail a low level of risk, once they fulfil their main function. The ALARP approach is described by the following Safety Assessment Principles paragraph:

- Paragraph 93: 'To demonstrate ALARP has been achieved for new facilities, modifications or periodic safety reviews, the safety case should:
 - i) identify and document all the options considered;
 - ii) provide evidence of the criteria used in decision making or option selection; and
 - iii) support comparison of costs and benefits where quantified claims of gross disproportion have been made.'

4.10.2.5.2 Selection of the Pyrotechnic Concept

345 The squib valve Summary Report (Ref. 69) is supposed to gather notable arguments and evidence to justify the choice of the squib valve design, including the pyrotechnic concept. However, this Summary Report mentions only one alternative pyrotechnic solution: [REDACTED]

346 In the report, Westinghouse states that this attempt was abandoned because of many issues. In the pyrotechnic cartridges development report (Ref. 96), Westinghouse state that 'alternative concepts for valve function, including the [REDACTED], were discussed at a meeting in June 2007; [REDACTED]

[REDACTED]. To date, the supporting document referred to in the Summary Report has not been transmitted (#35 (APP-PV70-GER-001)).

347 I consider that this document has the potential to provide evidence of optioneering to support the squib valve concept and should be transmitted to ND. I consider that this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall issue document (#35 (APP-PV70-GER-001)).

4.10.2.5.3 Selection of Propellants

348 In May 2010 I indicated to Westinghouse that the propellant selection process shall be ALARP. TQ-AP1000-704 (Ref. 10) was raised early June to formalize the query.

- 349 Subsequently I discussed the ALARP demonstration structure with Westinghouse during a technical meeting in July 2010; Westinghouse stated that such analysis was new for them.
- 350 TQ-AP1000-704 response was discussed during a technical meeting held in October 2010. Westinghouse committed to describe the propellant selection process, and to provide the ALARP argument and evidence, in the next revision of the Summary Report (Ref. 69). This revision was transmitted to ND on 31/12/2010.
- 351 In the Summary report (Ref. 69), Westinghouse states that:
- The sub-vendor UPCO chosen by SPX has developed the actuator for the previously-designed large valve for General Electric (GE) for their future use in Nuclear Power Plants.
 - The cartridge propellant was selected for historical reasons. It was used in the squib valve built for a previous US Department of Energy (DOE) project that had been subjected to similar radiation and thermal environments during its qualification testing.
 - P1 is the most common propellant used in aerospace industry; it has been shown to survive exposure to nuclear reactor environments.
 - P2 has been selected because the alternative more powerful and more characterized propellants used commonly in military and aerospace applications had an unknown stability under exposure to nuclear reactor environments.
 - An identified supplier UPCO has formulated and manufactured P2 originally for GE BWR prototype squib valves.
 - A large number of cartridges were exposed to thermal and radiation environments without degradation.
 - Alternative solutions consisting of testing the ability of off-the-shelf propellants would have had serious cost and schedule impacts.
- 352 I can understand that it is pragmatic and cost effective to use propellants already designed in the past for a similar project. However, the fact that both sub-vendor and propellant selections have been driven specifically to use former GE project propellants within the AP1000 design, does not provide adequate arguments that the selection has considered a sufficient range of options. I consider that there are other suitable pyrotechnic materials which have not been reviewed by Westinghouse.
- 353 Moreover, I consider that the rationales adopted to select P1 and P2 appear to be different: P1 has been selected because it is the most commonly used substance in the aerospace domain and it withstands nuclear reactor environment exposure tests; whereas P2 has been formulated and selected because other commonly used substances' stability to withstand nuclear reactor environments had not been checked previously, and P2 had some nuclear testing pedigree. Thus the rationale used to select P1 favoured firstly the common usage and secondly the capability to withstand a nuclear environment; whereas the rationale used to select P2 favoured firstly the capability to withstand a nuclear environment and secondly the common usage. This difference in decision making priorities should be supported with further justification.
- 354 Regarding the P1 selection, transposing good practice from the aerospace domain to the nuclear industry might be considered relevant. The expectations of initiators are indeed very similar, not to say identical: firing exclusively on demand, but both environments are significantly different. Pyrotechnic components in aerospace environments generally experience significant vibrations, accelerations and temperature variations. Pyrotechnic
-

components in nuclear reactor environments are subjected to few mechanical loads, but to a steady average high temperature, a steady average high humidity and to a high level of radiation.

- 355 In the Pyrotechnic Cartridges Development Report (Ref. 96), Westinghouse adds that the formulation of P1 dedicated to AP1000 squib valves does not contain a binder. The two same main propellant components of P1 are also used in the National Aeronautics and Space Administration (NASA) standard initiator, as presented in NASA documents (Refs 97 and 98). But the NASA standard initiator propellant includes 5 %w of a polymer binder. One of these NASA documents (Ref. 97) relates to a cryogenic firing issue. Such an issue is not relevant for nuclear reactors, but the document states 'although removing the binder appeared to solve the cold temperature problem, it was deemed an unacceptable solution because of potential age life reduction and other unknown effects on the propellants.'
- 356 I note that Westinghouse has decided to do what NASA has declined to undertake. Westinghouse has not provided any justification for this decision.
- 357 Regarding exposure to nuclear reactor environments, I consider that test results should be provided for both P1 and P2, including the demonstration that the nuclear reactor environment considered is comparable to the AP1000.
- 358 The Summary Report (Ref. 69), Appendix C, provides a list of existing BWR nuclear plants in the world, equipped with explosively actuated valves. The report does not contain any evidence that P1 and P2 have been used in actual nuclear environments. Moreover, there is no information to allow a comparison of pyrotechnics used between BWR and AP1000 environments. In order to establish a useful comparison, Appendix C should be updated either to provide the comparison between pyrotechnics of existing nuclear plants and AP1000 design, or to explicitly state that Appendix C does not substantiate the pyrotechnic aspects.
- 359 The Summary report Safety Claim #3 states that 'Westinghouse has an in-depth understanding of the squib valves' design and has been involved in the complete development and design process'. I consider that Westinghouse should demonstrate this by providing clarification and justification regarding the design choice of propellant.
- 360 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the arguments and evidence regarding the following items:
- Justify why different rationales have been adopted to select the pyrotechnic substances for the initiator and booster.
 - Demonstrate why good practice from aerospace is relevant within nuclear plants.
 - Justify the removal of the binder; notably, a comprehensive and well-argued analysis and supporting evidence requires to be provided.
 - Provide results of radiation exposure of the propellants, and the demonstration that reference environments used in the past are sufficiently similar to the environment expected within AP1000 reactors.
 - The relevance of the Summary Report, Appendix C in substantiating the pyrotechnics aspects.
-

4.10.2.5.4 Selection of Electrical Initiators

361 The same pyrotechnic concept, a gas generator pushing a piston, may be initiated in several different ways. The electrical ignition that Westinghouse has chosen is one method.

362 I have asked Westinghouse for justification regarding the initiator ignition mode TQ-AP1000-704, (Ref. 10). They committed to provide an ALARP demonstration in the Summary report. Westinghouse states in the latest revision of this report (Ref. 69) that:

- Other concepts have been considered, which have been rejected by Westinghouse on the basis they were not '*expectable for the AP1000 design*' (sic):

i) [REDACTED];

ii) [REDACTED]

- The chosen electrical igniter has been extensively used because of its simple and reliable design, in military and aerospace applications.

(I have understood the word *expectable* used in the Summary Report (Ref. 69) to mean *suitable*).

363 The Summary Report does not provide evidence in respect of this non selection aspect. All the considered concepts should be documented in the Summary Report; notably, advantages and disadvantages of each concept should be provided. Furthermore, the criterion "expectable / not expectable" appears to be vague and should be defined more explicitly.

364 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall provide:

- A review of the advantages and disadvantages of each considered initiator concept.
- An explanation of the selection criterion for the initiator ignition concept.
- The analysis to support the selection of each considered initiator concept.

4.10.2.5.5 Selection of Electrical Current Values

365 Two specific electrical current values define electrical characteristics of initiators equipped with a bridgewire, such as those used for the AP1000 reactor. The so-called 'all-fire current': all initiators subjected to the all-fire current or more are expected to fire. The so-called 'no-fire current': none of the initiators subjected to the no-fire current or less is expected to fire.

366 Obviously, the no-fire current value reflects the electrical sensitivity of an initiator. A high no-fire value favours the initiator's ability to withstand without firing any spurious signals that a damaged command device might issue and any potential electromagnetic interference in the ignition lines that surrounding transmitters might induce.

367 The higher the no-fire current value is, the lower the initiator sensitivity is. I consider that the no-fire value of AP1000 design is not particularly high, given that the electrical features included within the C&I systems may be able to supply higher currents. I have questioned Westinghouse regarding this concern TQ-AP1000-1149, (Ref. 10).

368 In their response, Westinghouse has tried to justify the no-fire and all-fire current values by the fact that AP1000 initiators are very close to other initiators already designed for a

safety system of the [REDACTED]. However, the Summary report does not mention whether the [REDACTED] initiator propellant includes a binder. Westinghouse has stated that AP1000 requirements have been set by considering existing properties of the initiators previously designed for [REDACTED]. TQ-AP1000-1149 (Ref. 10) response appears to be based on the fact that using an already-designed initiator is a stronger justification than designing an initiator from scratch with a very low electrical sensitivity. Whilst I accept that pedigree is an important leg of a safety argument, this should also be relevant and should not exclude the use of better technical options.

369 Westinghouse has not provided any optioneering in respect with the choice of the initiator electrical properties and I consider there is insufficient justification that the choice of electrical current values provides a reduced level of risk, as the ALARP approach requires. In summary, I consider this to be part of the Squib Valve **GDA Issue (GI-AP1000-ME-01)**; Westinghouse shall provide:

- A review of the advantages and disadvantages of each considered electrical current value.
- An explanation of the selection criterion for the electrical current value.
- The analysis to support the final selection of each considered option.

4.10.2.5.6 Qualification of Cartridges

370 I have considered the relevant Equipment Qualification aspects related to the pyrotechnic cartridges.

- Safety Assessment Principle EQU.1 (Ref. 4) states 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'

371 In October 2010, a representative from UPCO provided an updated overview of pyrotechnic parts' design. Originally, this overview had been provided during the Intermediate Design Review.

372 During the meeting, Westinghouse stated that the detailed information related to the pyrotechnic parts' design is captured in the Ballistic Report. Regarding the details of actuator development, the Summary Report (Ref. 69) refers to the Ballistic analysis report; but it appears that this document is neither numbered, nor transmitted yet.

373 On the 21 February 2011, Westinghouse transmitted to ND the Development Report regarding the pyrotechnic cartridges for AP1000 squib valves (Ref. 96). It appears to deal with items expected in a ballistic report but it is not actually presented as such.

374 I consider that this to be part of the Squib Valve **GDA Issue (GI-AP1000-ME-01)**; Westinghouse shall clarify the relevance and purpose of Development Report (Ref. 96) to the ballistics analysis.

375 The previous revision A of Pyrotechnic Actuator Requirements (Ref. 65) planned an X-ray and an N-ray test on a cartridge, (an N-ray test is a neutron radiation exposure). Like the X-ray test, the N-ray test was initially proposed to check that internal components are properly positioned; it was not to check the propellant stability under neutron radiation. Subsequent Westinghouse documentation has removed the specification for an N-ray test, but I now understand that this will be reinstated (albeit not with the same objective).

376 The documented qualification programme (Ref. 89) for the squib valve actuators includes a radiation test, based on the estimated location of each room where squib valves will be

positioned. The test is planned to be performed only with gamma radiation, from a Cobalt-60 source. Beta and neutron components included in the actual radiation environment are modelled by a gamma equivalency using a coefficient between dose rates.

377 Inside the containment and away from the RPV, neutron component radiation is not the main one. But explosive substances frequently include significant fractions of relatively light natural elements, which are sensitive to neutron radiation. I have questioned Westinghouse regarding the justification of the gamma equivalency coefficient because although the coefficient is higher than 1, its value is slightly lower than those recommended for living tissues, as a comparison TQ-AP1000-1150, (Ref. 10).

378 The Westinghouse response was not supported by any argument or evidence. Nevertheless, it indicated that it was planned to subject propellants to neutron testing as part of the equipment qualification, which eliminates this concern. Adding a new test dedicated to neutron radiation in the qualification programme is in line with my expectations.

379 In December 2010, Westinghouse advised the test parameters will only be finalised at a future date.

380 In summary, I consider that some items mentioned above are part of the Squib Valve **GDA Issue (GI-AP1000-ME-01)**; Westinghouse shall generate and issue the following documentation:

- Finalised requirements regarding the propellant neutron testing, by justifying the energy, the intensity, and the duration of exposure.
- Qualification results, which includes the substantiation that actuators as proposed are adequate to achieve their safety functional requirements and their design intent.

381 Cartridges with P1 and P2 have been used for all the seventeen tests performed for the AP1000 design. Some of the tests were representative of worst expected conditions in the range of design parameters. Valves have been opened each time. This outcome proves that cartridges are fully able to fulfil their main function of supplying a sufficient amount of energy on demand. However, there has been an apparent paradox between two different tests for the same type of valve, regarding the correlation between piston velocity and booster charge load: the piston velocity was a little bit lower for a test although its charge load was significantly higher than in the other test.

382 I have requested clarification from Westinghouse TQ-AP1000-1148, (Ref. 10) regarding this question. Westinghouse has responded that:

- Firstly, both these tests were parts of Testing Round 1, which used a rather low-accuracy system to measure the piston velocity. A further analysis performed later has tended to reduce the velocity gap. This argument regards all Round 1 tests.
- Secondly, variations could result from the P2 granule size and the tension bolt breaking strength. Controls of both variables have been improved after the Intermediate Design Review, for the Round 1 extension and the Round 2 tests.

383 The tension bolt breaking strength is not pyrotechnic-related. I note that Westinghouse's response did not refer to the pressure curves, although pressure fronts and peaks of both considered tests appear to reflect roughly and qualitatively the difference of initial charge load. Thus, pressure curves do not show the same paradox as velocity measurements do. This tends to confirm that the variability in results is due to the tension bolt breaking strength. However, the importance of P2 granule size is to be noted.

-
- 384 Westinghouse and their vendors decided to change some design features after the first round of tests, leading to a significant reduction in the P2 charge load in each type of valve. I have assessed from a pyrotechnic perspective the results of the sixteen tests (noting the issue re recording equipment for one test) provided in the Test Report (Ref. 70). The lower pressure at shear cap / piston impact can indeed be noticed.
- 385 From my assessment I consider that propellant mass, pressure peak value, pressure at impact, and piston velocity at impact are a coherent set of technical parameters. Moreover, for two groups of four tests performed in similar conditions, (the propellant mass is the variable parameter) the correlation between pressure peak value and charge load is reasonable.
- 386 The qualification programme (Ref. 89) plans to qualify cartridges in thermal ageing. It does not address any humidity ageing. However, the leakage rate required by specifications is higher than zero. Thus I have questioned Westinghouse regarding the potential degradation of propellant due to moisture ingress TQ-AP1000-1149, (Ref. 10).
- 387 Westinghouse has provided a comprehensive calculation in the Summary Report (Ref. 69). They conclude that moisture ingress would likely have no significant consequence, due to the fact that P1 is non hygroscopic, that water will not easily ingress into a cartridge because of its strong surface tension, and that cartridges are located inside squib valve body most of time.
- 388 I consider that this analysis is satisfactory and I have not identified any concerns associated with this area.
- 389 I have assessed the Squib Valves Failure Modes and Effects Analysis (Ref. 45) from a pyrotechnic point of view. I have determined that:
- There was no mechanical shock of cartridges addressed.
 - There was no difference between 8 inch LP and 8 inch HP squib valves.
- 390 I have subsequently questioned Westinghouse TQ-AP1000-706, (Ref. 10) regarding this matter. In October 2010, Westinghouse recognised that:
- Cartridges were not qualified to withstand dropping.
 - The 8 inch LP and 8 inch HP valves are not diverse, from a pyrotechnic perspective, although they have different propellant charge quantities.
- 391 I consider the first item mentioned above to be part of the Squib Valve **GDA Issue (GI-AP1000-ME-01)**; Westinghouse shall identify in the safety case that every cartridge subjected to a significant mechanical shock loading during its lifetime must not be used, as a safety requirement. As part of this, Westinghouse should define the acceptance parameters in respect of this criterion.

4.10.2.5.7 Reliability Claims – Pyrotechnic Components

- 392 I have considered the relevant Reliability Claims aspects related to the pyrotechnic cartridges.
- Safety Assessment Principle ERL.1 (Ref. 4) states ‘The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.’

- Safety Assessment Principle ERL.2 (Ref. 4) states 'The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.'

393 Westinghouse has selected squib valves arguing their reliability is better than the other type of valves, such as motor-operated and air-operated. In order to justify its selection, Westinghouse has issued a document called Squib Valve Modelling in the AP1000 PRA (Ref. 92), which contains the main results of [REDACTED] analysis and a technical memorandum produced by [REDACTED] re the reliability of pyrotechnically actuated valves. This documentation refers to thousands of tests having been performed. The reliability comparison is now presented in the Summary Report (Ref. 69) more formally.

394 In June 2010, based upon the documented Squib Valve Modelling in the AP1000 PRA, I have questioned Westinghouse regarding the relevance of such results to the AP1000 design cartridges TQ-AP1000-724, (Ref. 10). I consider AP1000 pyrotechnic components have to be close enough to those actuated in the past to take benefits of the thousands of tests for the reliability claims.

395 The reliability estimate is supported by past actuations of [REDACTED] valves, [REDACTED] cartridges, [REDACTED] valves, [REDACTED] cartridges, and about [REDACTED] other valves. Considering such numbers, it is not questioned that the pyrotechnic reliability of initiators is established in principle. But to date, Westinghouse has not detailed all the potential differences between AP1000 design initiators and all those fired in the past. However, to substantiate the reliability claim, Westinghouse should provide adequate arguments and evidence that the proposed AP1000 initiator design is comparable to those already tested, notably in terms of propellant recipe and bridgewire properties. I consider that too many or too important differences would undermine the reliability relevance and would necessitate further justification.

396 [REDACTED] have based their analysis on [REDACTED] valves from military applications. However, the [REDACTED] tested valves did not include any booster. The memorandum from [REDACTED] describes the type of valves tested. It is a 5-inch valve developed for a US military project. It contains one sole initiator because the energy released in the burnt gas of one initiator is sufficient to push the small piston and open the valve. Thus, the [REDACTED] tested cartridges did not include any booster. It is called cartridge in the text of the memorandum, though there is no booster.

397 The Summary Report (Ref. 69) refers to [REDACTED] cartridges. But it does not mention which type of cartridge it is: with initiators only, or with initiators plus booster.

398 The Test Report (Ref. 70), Appendix B is the sensitivity analysis of the AP1000 squib valve. Regarding the function 'Generate pressure' within the squib valve opening sequence, the sensitivity analysis identifies eight variables. Six of them concern directly the booster (like the aforementioned granule size), none of them concerns initiators. Moreover, the AP1000 design booster contains the propellant P2 in a particular 2-form structure, which may reduce the number of past tests to which the AP1000 design might be judged similar.

399 I consider necessary that the pyrotechnic reliability demonstration focuses on the booster. Definitely, there is confusion in the use of the word cartridge, between the way it is used in the memorandum of [REDACTED] and the one by Westinghouse, as it is defined in Pyrotechnic Actuator Requirements (Ref. 65). The Summary Report does not clearly

provide adequate arguments and evidence to support the claimed reliability for the booster designs.

400 In summary, I consider that items mentioned above are part of the Squib Valve **GDA Issue (GI-AP1000-ME-01)**; Westinghouse shall generate an argument that demonstrates that:

- Test data from carrying out initiator tests by others provides suitable reliability evidence for use with the AP1000 design given the variance in the AP1000 initiator design and the use of a binder.
- Sufficient and relevant test evidence exists for the AP1000 booster design to support its reliability claim.

4.10.2.5.8 Reliability Claims – Electronic Ignition Circuits

401 My assessment has also covered Electronic Ignition Circuits (EIC) which is connected on each initiator. There is one initiator PMS and one initiator DAS on each squib valve; there is a second PMS initiator on each ADS stage 4 squib valves. There are therefore twenty-eight initiators (16 PMS and 12 DAS) and thus twenty-eight EICs. PMS and DAS EICs are supposed to be different because Westinghouse has organised two different teams to design each EIC type separately, in order to promote diversity.

402 All EICs have to be designed to allow the same 4-step sequence to fire initiators:

- ARM: when the ARM signal is issued, the relevant circuit begins to be fed;
- HOLD: the circuit must be fed during a short specified duration;
- RELEASE: the circuit must be de-energised before;
- FIRE is energised, thus delivering the energy stored during HOLD step.

403 Moreover, the FIRE signal must be commanded within 30s after RELEASE has been commanded. This means that the circuit must be able to supply a current value at the all-fire current of initiator, or more. After 300s following RELEASE, the circuit current must have bled down to the no-fire current value.

404 The reliability of the squib valve system should obviously take into account the EIC reliability. In May 2010, I questioned Westinghouse to get information regarding the description of the device, its reliability, its qualification programme and the mitigation arrangements planned to address any failure mode of the components. I formalised my queries early June 2010 TQ-AP1000-718, (Ref. 10).

405 Westinghouse has not responded clearly regarding the qualification programme. They have responded that there are no particular mitigation means to counter a component failure, apart from EIC redundancy and environment measures to reduce harsh conditions, such as a double housing, and some environmentally controlled spaces.

406 The response is supported by three documents, including AP1000 Standard Safety System squib Valve Termination Unit Assembly Hardware Requirements Specifications (Ref. 93). This document contains PMS termination unit requirements. The requirement R28-2 specifies the Mean Time Between Failure (MTBF) but currently, the latter is 'TBD', which I interpret to mean 'To be defined.' Westinghouse's response stated that the MTBF should be more than 40 years, presenting that result as a performance of the designed PMS termination unit.

- 407 The other two documents are Design Reports regarding the PMS termination unit and its capacitor bank prototype. The design solution uses resistor-capacitor circuits. Capacitors are charged during the HOLD step and begin to discharge from RELEASE event. But the requirement of a current higher than all-fire value during 30s imposes electronic characteristics to the discharge capacitor and resistor incompatible with the relatively rapid discharge to a current lower than no-fire current after 300s. Hence, the Test Report for PMS termination unit proposes a design change, consisting in extending the 300s requirements to 1500s.
- 408 In October 2010 I questioned Westinghouse as to whether the MTBF would change if the design should be made again to meet its requirements. Westinghouse has responded that the MTBF would not change. I was then informed that the response to TQ-AP1000-718 only concerned PMS, although my original query intention covered both the PMS and DAS.
- 409 Then I raised two new queries, one dedicated to each PMS and DAS system, respectively TQ-AP1000-1147 and TQ-AP1000-1152 (Ref. 10). In TQ-AP1000-1152 response (DAS), Westinghouse stated that the MTBF would be more than 88 years (1.29 failure/10⁶ hours).
- 410 Westinghouse has now confirmed that the design of EICs will not be finalised before May 2011.
- 411 I consider that EICs are key elements in the squib valve system and may have a significant impact on overall reliability. To date, it has been impossible to assess them properly because their design is not finalised and my queries lead to confusion between requirements and actual performance.
- 412 In summary, I consider that items mentioned above are part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the justification that each squib valve EIC type is designed adequately to achieve its safety functional requirements and its design intent. This justification shall include:
- The comprehensive list of safety and functional requirements, including surveillance, monitoring requirements.
 - The detailed description of design solutions.
 - The qualification programme and its results.
 - The description of EMIT provisions required to maintain safety functions.

4.10.2.5.9 Spurious Actuation

- 413 I have considered the risk of spurious operation related to the squib valves.
- Safety Assessment Principle ESS.22 (Ref. 4) states 'A safety system should avoid spurious operation at a frequency that might directly or indirectly degrade safety.'
- 414 Although pyrotechnic substances are under consideration, the squib valve actuation is not a dangerous explosive event in itself, because propellants used are not high explosives and the energy released is held within the valve body. Nevertheless, if a cartridge would deflagrate out of the valve, for instance during its replacement, it might provoke serious injuries and casualties.
- 415 Regarding nuclear safety, the spurious actuation of squib valves has to be considered as the loss of their isolation function (containment safety function). In case of a spurious opening of an IRWST injection squib valve, some check valves would prevent the

depressurisation of the primary circuit towards the IRWST. Recirculation squib valves are not linked directly to the primary circuit; their spurious opening would not lead to a reactor depressurisation. On the other hand, a spurious actuation of one of ADS-4 valves leads to a rapid depressurisation of the primary circuit leading to a LOCA.

- 416 In the pyrotechnic perspective, it appears that several events might lead to a spurious actuation: for example signal currents might be sent unintentionally to one or more initiators. Electrical currents could also be generated in situ between the ignition wires and the initiators, due to environmental electromagnetic fields. My assessment of this specific case is presented below in the section covering Electromagnetic Interference (EMI) sensitivity. The thermal environmental conditions might also act directly onto the propellants. However, most spurious actuation scenarios involve the initiators. The ADS-4 valves represent 33% of all squib valves and 43% of all initiators, which is important to note since the spurious actuation frequency is influenced by the number of initiators per valve, which is greater for the ADS4 valves.
- 417 Propellants P1 and P2 have a temperature threshold of auto-ignition; P1 (initiators) auto-ignition temperature is lower than the one of P2. A scenario of fire within the containment might reach the threshold for P1 auto-ignition, which would lead to valves opening, notwithstanding consequences on safety due to the fire. I have questioned Westinghouse regarding this scenario TQ-AP1000-826, (Ref. 10).
- 418 TQ-AP1000-826 response shows a significant margin below the auto-ignition temperature. The method applied has consisted in calculating the peak temperature incurred during a postulated fire occurring in the room where squib valves are located. The fire duration was taken as described in the fire protection analysis within the AP1000 European Design Control document (Ref. 88, Appendix 9A). The squib valve initial temperature was the one resulting from calculations addressing the presence of the hot coolant fluid inside the valve shear cap.
- 419 These calculations have been performed for the former design of ADS-4 squib valves, where cartridges were positioned on the top of the valve bonnet and formed part of the valve pressure boundary. In the current design, cartridges are embedded inside the bonnet: they no longer form part of the valve pressure boundary, and are less susceptible to the room environment, thus the initial temperature is considered to be slightly higher than the one used in the analysis.
- 420 The fire duration in rooms where ADS-4 squib valves are located is short (Rooms B and C). Room A adjoins Room C; they are separated by a concrete wall. Moreover, the ceiling of Room A is located at the level of Room C. Therefore, a heat build-up in Room A might generate a significant temperature in Room C. And yet, the fire duration for the fire zone including Room A is the longest within the containment. However, the concrete wall thickness is more than one foot (305mm), Room C is open (no ceiling) and squib valves are situated behind the steam generator from the common wall. This scenario is therefore likely to be more onerous than that which has been analysed, but still lower than the auto-ignition temperature with sufficient margin.
- 421 In summary, the analysis performed to date cannot be regarded as conservative. The current analysis is based on the squib valve former design, and it does not consider adjacent rooms within the containment. I consider this to be part of the Squib Valves GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue a further analysis to confirm that, in case of a fire in adjacent containment fire zones, the present design of cartridge peak temperature is maintained below the propellant auto-ignition temperature with an adequate margin.

- 422 Early January 2010, I questioned Westinghouse regarding safeguards selected for the AP1000 design in the pyrotechnic domain, to reduce the spurious opening probability (TQ-AP1000-435, Ref. 10). In March 2010, Westinghouse responded that 'From a safety perspective it is equally important that the squib valves do not open when they are not intended as it is that the valves do open when they are intended.' This statement indicates that there is no fail-safe position of ADS-4 squib valves. Westinghouse also responded that safeguards are the firing 4-step sequence (previously described), the absence of power in the squib valve cabinet until an ARM command is issued, and the cable segregation.
- 423 I subsequently asked for detailed information regarding EICs. As previously described, I have not yet received this information. In the Summary Report (Ref. 69), Westinghouse states 'The squib valves and the associated firing logic have been designed to achieve extremely low probabilities of spurious actuation. See Appendix G for additional discussion and supporting evidence. Additionally, this area has been the subject of extensive regulatory review by both the NRC and the ND.' (Safety claim 2, argument 2.4). Appendix G has been included in the last revision of the Summary Report (31/12/2010). It is dedicated to the spurious actuation prevention of the ADS-4 squib valves; it describes the qualitative principles required for EICs design and for associated C&I systems.
- 424 Due to the shortfall of detailed information regarding EICs and the late issue of Appendix G, I have not been able to undertake my planned assessment in this area.
- 425 According to Appendix G, spurious actuation is prevented by:
- Cabling measures: interconnection between initiator circuits is prevented, raceways are shared with circuits in which currents are lower than the no-fire value;
 - There is normally no power source in EICs, except in case of signal from cabinet interface modules;
 - The firing process uses the particular ARM / HOLD / RELEASE / FIRE sequence described above;
 - ARM and FIRE signals are sent from different cabinet interface modules, which are physically separated.
- 426 I consider the cabling measures constitute an adequate passive safeguard to reduce the number of scenarios liable to generate a spurious squib valve firing. I note that all the active provisions against inadvertent actuation nevertheless exclusively rest with EICs and cabinet interface modules within PMS, upstream the squib valve cartridges.
- 427 Regarding the relevance to the UK of US standards used in the AP1000 design, TQ-AP1000-703, (Ref. 10), Westinghouse has responded notably the following paragraph (partly from the HSE SAPs):
- 'Engineering principle ECS.4 (Ref. 4) states that "For structures, systems and components that are important to safety, for which there are no appropriate established codes and standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied." In line with the recommendations given in ECS.4, standards issued for similar equipment used for military equipment (vehicles, missiles, satellites, etc...) and thus with similar safety significance have been used and adapted for the AP1000 squib valves.'

- 428 I have considered the US military standard MIL-STD-1316E (Ref. 46), which is approved for use by all departments and agencies of the US Department of Defence, and deals with safety criteria for fuse design. This standard provides definitions, including the following ones:
- Armed: A fuse is considered armed when any firing stimulus can produce fuse function.
 - Dud: A munition which has failed to function, although functioning was intended.
 - Enabling: The act of removing or activating one or more safety features designed to prevent arming, thus permitting arming to occur subsequently.
 - Explosive train: The detonation or deflagration train beginning with the first explosive element and terminating in the main charge.
 - Fuse safety system: The aggregate of devices included in the fuse to prevent arming and functioning of the fuse until a valid launch environment has been sensed and the arming delay has been achieved.
 - Safety feature: An element or combination of elements that prevents unintentional arming or functioning.
- 429 It also provides requirements, notably the general requirement 4.2.1 Safety redundancy, which states ‘The safety system of fuses shall contain at least two independent safety features, each of which shall prevent unintentional arming of the fuse. The stimuli enabling a minimum of two safety features shall be derived from different environments. (...)’. This principle prevents any single stimulus firing an initiator, then conducting to the main charge, by using two independent safety devices.
- 430 Military weapons commonly include several safety features, which are calibrated to switch (enabling) from specific environmental variable thresholds, which are representative of the expected operational process environment. Furthermore, the safety principle required in MIL-STD-1316E is also used frequently for military systems that are not fuses in the strict sense of the word, by adding Safety and Arming Devices (SADs). Those are not environmentally driven but they participate efficiently in reducing the spurious firing probability. Adding safety and arming devices within explosive trains is a standard requirement for munitions but also a good practice in rocket design.
- 431 The squib valves are not weapons but the analogy is easy to draw: the explosive train would be the cartridge, including initiators and the booster; initiators would be a part of detonator, and the booster would be the main charge. The AP1000 design contains no safety feature inside the explosive train and cannot comply with the standard principle. Within AP1000 design, except for particular failure cases, each initiator firing leads to a valve opening. In the logic of MIL-STD-1316E, it is permanently “armed”. The AP1000 design needs not comply strictly to the military standard. However, in accordance with SAP ECS.4, and the relevant statement of Westinghouse, I consider it to be a reasonable expectation that squib valve explosive trains should include SADs, as required by MIL-STD-1316E, or their absence should be explicitly justified.
- 432 Standard requirements for adding SADs ensure that there is a fail-safe position for weapons. It is indeed commonly preferred, at least for NATO member countries through STANAG 4187 (Ref. 103), that a weapon is dud rather than exhibits a high risk of spurious blast. However, such a preference cannot be easily transposed to squib valves, where firing and actuation performs an important safety function.
-

- 433 Adding SADs within the pyrotechnic train makes the probability of squib valve failure to open on demand higher, due to the inherent reliability (i.e. probability of failure) of SADs themselves, but as a consequence their use would decrease the probability of spurious actuation. Decreasing the probability of the inadvertent opening event can only be obtained by increasing the probability of failure to open on demand, and vice versa. There are therefore symmetric constraints in respect of both competing events, and the final design decision will need to be a justified compromise.
- 434 Thus, the lack of SADs within the pyrotechnic train should be justified by the need for high reliability of the intentional opening, balanced against the risk of spurious firing.
- 435 It is understood that, the primary circuit exhibits a global (small) probability of LOCA, to which the particular event of ADS-4 squib valve spurious actuation contributes. Large component design and manufacturing quality contributes also to this probability. But the specific contribution due to the squib valve spurious actuation must not be too high in comparison with the other LOCA contributors, (e.g. associated with the break preclusion concept and weld in-service testing on the main loop circuit). Too high a probability of ADS-4 spurious actuation would perhaps justify reducing the reliability requirement of opening on demand, by adding SADs within the pyrotechnic train for example.
- 436 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the comprehensive justification that:
- Safeguards that are required (the design is not completed yet) within the EICs and cabinet interface modules are sufficient to reduce the spurious actuation probability at a level coherent with other potential sources of LOCA.
 - The absence of SADs within the pyrotechnic chain achieves the correct balance between the two competing demands of preventing spurious actuation of the squib valves, and yet ensuring they have a high reliability of operating on demand to support the passive core cooling function.

4.10.2.5.10 Electromagnetic Interference (EMI) Sensitivity

- 437 I have considered the risk of electromagnetic interference related to the squib valves.
- Safety Assessment Principle EHA.10 (Ref. 4) states 'The design of facility should include protective measures against the effects of electromagnetic interference.' And its related paragraph 223 states 'An assessment should be made to determine whether any source of electromagnetic interference either on-site or off-site could cause malfunction in or damage to safety-related equipment or instrumentation.'
- 438 Electrically actuated initiators are sensitive to EMI. Their bridgewire is connected to wires and this set behaves as an antenna, like all conductor material placed in electromagnetic fields: induced currents generate in wires and thus in the bridgewire. If the current value exceeds the no-fire value of an initiator, it may fire.
- 439 I have questioned Westinghouse regarding EMI sensitivity TQ-AP1000-437, (Ref. 10). They have responded that outside of operating conditions (transportation, storage), cartridges will be contained in a safety fixture designed to protect personnel from exposure to cartridge output pressure; and initiator pins will be linked with a shorting spring. During operation, the cartridge will have connectors and shielding wiring that have been qualified for electromagnetic conditions per APP-PV70-T5-002, Electromagnetic Interference (EMI) Test Procedure for a Squib Valve Initiator and a Connector Assembly (Ref. 90).

- 440 I noted that the EMI test procedure (Ref. 90) does not look specifically for the resonant harmonics but consists in checking the functionality of the set connection plus initiator during and after an exposure to different ranges of frequency and electromagnetic fields. I have requested Westinghouse to inventory all field sources that initiators may be exposed to. I have also requested them to provide arguments and evidence that the design process has captured such electromagnetic environments TQ-AP1000-705, (Ref. 10).
- 441 Westinghouse's response was a list of standards and guidance prescribed by US NRC Regulatory Guide 1.180. This list simply matched the EMI Test Procedure (Ref. 90). I consider the maintenance requirements for EMI protection should also be adequately defined.
- 442 In October 2010, I indicated to Westinghouse that my query was not "How are you complying with US NRC Regulatory Guide 1.180?" but "Has the design process actually captured all the electromagnetic environments that initiators will be exposed to?" I consider that such query is all the more necessary since there is no safety feature within the explosive train and the no-fire current value is not high.
- 443 Westinghouse subsequently presented a calculation of the necessary power to induce a current of the no-fire value in a dipole antenna. The result is a huge power, which is not realistic for transmitters liable to be used inside the containment or in surroundings.
- 444 I consider that the calculation method is not sufficient to demonstrate the non susceptibility of initiators to EMI. I recognise that neglecting shielding and the cable protection is a strongly conservative assumption for operating conditions. However, I consider that a dipole antenna with a resistance of 73Ω is not representative of the actual AP1000 ignition circuit and the inverse square law of distance starting from the receiver, as used in the calculation of Westinghouse, is less accurate than a calculation of equivalent isotropically radiated power (EIRP) and subsequent electromagnetic fields from a postulated transmitter.
- 445 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the justification that:
- Cartridges will not be liable to react to any electromagnetic environments, with adequate consideration to resonant harmonics that they will be exposed to throughout their life cycle.
 - EMIT requirements for EMI protection is suitable and adequate.

4.10.2.5.11 Pyrotechnic Surveillance and EMIT

- 446 For this item, I have considered the following Safety Assessment Principles:
- Safety Assessment Principle EMT.1 (Ref. 4) states 'Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.'
 - Safety Assessment Principle EMT.5 (Ref. 4) states 'Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.'
 - Safety Assessment Principle EMT.6 (Ref. 4) states 'Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals throughout plant life commensurate with the reliability required of each item.'

- Safety Assessment Principle EMT.7 (Ref. 4) states 'In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.' And its related paragraph 193 states 'Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.'
- Safety Assessment Principle EAD.3 (Ref. 4) states 'Where material properties could change with time and affect safety, provision should be made for periodic measurement of the properties.'

447 My assessment covers EICs, cartridges and electrical wires between them. The case of EICs will be addressed as part of the GDA Issue, as discussed previously. The case of shielding of cables will be addressed as part of the GDA Issue regarding electromagnetic interference.

448 Regarding cartridges, Westinghouse has decided to apply the ASME code, ISTC-5260 (Ref. 102) regarding explosively actuated valves. It requires notably that:

- Each charge cannot be used for more than ten years.
- At least 20% of the charges shall be fired and replaced at least every two years.
- If a charge fails to fire, all charges with the same batch number shall be removed, discarded, and replaced with charges from a different batch.
- Replacement charges shall be from batches from which a sample charge shall have been tested satisfactorily.

449 According to In-service Recommendations (Ref. 68), 'one cartridge from each valve type will be tested each outage.' There are four types of valves (14 inch ADS-4, 8 inch LP, 8 inch HP Right, 8 inch HP Left) and an outage should occur every eighteen months. Moreover, in the documented qualification programme (Ref. 89), the thermal aging test considers operational life duration of 8 years. I consider therefore that these provisions meet the two first requirements of ISTC-5260.

450 For all AP1000 licensees concerned by ASME requirements, as in the UK, it is necessary to know how to perform cartridge testing and how to consolidate results. Moreover, they have to be informed that they may need to shutdown their Nuclear Power Plant, in order to replace cartridges that come from a batch from which a cartridge has recently failed to fire properly for another utility. During a technical meeting of October 2010, an UPCO representative indicated that the manufacturing facilities of P2 propellant were dedicated to avoid undesirable contamination from another propellant, and that bigger batches tend to reduce cartridges cost. Nevertheless, licensees may choose not to share their batches with other Nuclear Power Plants or other licensees (as a commercial decision).

451 Since they impact on cartridges' functionality, the arrangements for testing and batch management are safety requirements. Applying SAP EMT.1, I consider these requirements should be identified in the safety case.

452 I have questioned Westinghouse regarding the cartridge testing and batch management, TQ-AP1000-1153, (Ref. 10). Westinghouse has responded: 'The safety case assumption that if a cartridge taken out of a plant fails its test then all cartridges from that batch should be replaced, will clearly be identified in Chapter 17 of the PCSR (March revision) and in the squib valve summary report.' This is presently only captured within the Summary Report (Ref. 69). I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall explicitly capture in the consolidated PCSR the

requirement that if a cartridge taken out of a plant fails its test then all cartridges from that batch should be replaced.

- 453 The complete testing of an explosively actuated valve is not adequate because it is a one-shot device. Electrical continuity and insulation of electrical wires between EICs and initiators should be tested to clear every risk of signal loss from EICs. I have questioned Westinghouse on this item, in January 2010 TQ-AP1000-438, (Ref. 10), in June 2010 TQ-AP1000-720, (Ref. 10) and in November 2010 TQ-AP1000-1164, (Ref. 10). The first two responses were not adequate. During a technical meeting of December 2010, Westinghouse agreed to transmit the design intents and the procedure philosophy of this testing.
- 454 Westinghouse finally transmitted the whole procedure CPP-PMS-GJP-813 Engineered Safeguards Actuation System 24-Month Actuation Device Test (Ref. 95), although it is a document under the operator responsibility. I have not reviewed all the procedure because it is partially out of the GDA assessment scope; I have however identified the following arrangements as design intents extracted from the procedure:
- The testing is performed every 24 months.
 - There is no insulation testing.
 - The continuity testing is performed with a digital voltmeter.
 - Ignition lines are reconnected on initiators while they are fed by the voltmeter (in ohmmeter mode).
- 455 Considering their safety function, squib valves need to be maintained at a high level of availability. I recognise their complete pyrotechnic system testing is not practicable. I consider that a single test performed only every 24 months might be sufficient, provided that it can be ensured that there will not be any changes in the squib valve's environment until the next test. This requires prevention of access to rooms where squib valves, EICs, and cable raceways between both are located; this appears to be patently not practicable. In response to TQ-AP1000-719 (Ref. 10), I noted that Westinghouse has mentioned that, for aircrafts, the continuity is checked 'either continuously or periodically.' (AP1000 squib valves' initiators are derived from [REDACTED] initiators, as discussed previously).
- 456 With each initiator containing two connecting pins, I considered it is possible that during their assembly, the connecting plug could appear to be correctly aligned, when in fact it is possible for a pin to bend and come into contact with the adjacent pin. As a result the bridgewire is short-circuited. In this scenario, it is not possible to guarantee adequate current to the bridgewire. I therefore consider a need to collate adequate evidence that this scenario is either eliminated by design, or that a connection defect is clearly detectable.
- 457 There is no particular requirement on the digital voltmeter. On ohmmeter mode, off-the-shelf voltmeters supply a current from their internal battery and set by the output resistor. It may supply a current higher than the maximum value allowed during the non-destructive bridgewire resistance test, performed in lot acceptance testing.
- 458 It is known as not a good practice to connect together fed circuits.
- 459 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the justification that electrical testing EMIT requirements result from a process which has considered and analysed each option, with

a suitable selection rationale. This justification should demonstrate specifically the following items:

- Testing every 24 months is sufficient to prove a high level of availability of the safety system using squib valves.
- Insulation testing does not reduce the risk of failure.
- Electrical currents supplied by digital voltmeters always stay lower than the threshold defined in bridgewire resistance test.
- Reconnecting initiators to a circuit under voltage does not increase the risk.

4.10.2.5.12 Lot Acceptance Destructive Tests

460 Each lot of initiators and boosters is subjected to acceptance testing, including destructive and non destructive tests; 10% of a lot are subjected to destructive tests. Originally, the destructive tests for initiators were no-fire, continuity and all-fire tests. No-fire and all-fire test consist in exposing initiators respectively to the no-fire or all-fire current to check that the behaviour of initiators meet the requirements. The continuity test consists in exposing initiators to the expected current going through the bridgewire during continuity check. Tests are planned to be performed in the following order: no-fire, continuity and all-fire.

461 I recognise that all-fire test is undoubtedly destructive and must be performed last of all. On the other hand, the no-fire and continuity test must not affect initiators' properties, and specifically, their ability to keep meeting no-fire and all-fire requirements.

462 This subject has been discussed during a technical meeting in October 2010 and I raised a query to formalise my concerns TQ-AP1000-1151, (Ref. 10). I have specifically asked Westinghouse regarding the impact of repeating the no-fire and the continuity test on bridgewire properties.

463 In January 2011, Westinghouse has responded that the continuity test will be removed from the specification. It has also stated that the no-fire will not be repeated during the operation phase because the no-fire test is always and only performed before all-fire one.

464 Regarding the continuity test, the test procedure (Ref. 95) indicates that a current supplied by a digital volt meter will go through the bridgewire. Moreover, the procedure implementation is planned to be repeated. Thus, it must be checked that the continuity test is actually not destructive, even if it is not absolutely necessary to formalise it as a non destructive test for lot acceptance. This concern is captured by the GDA Issue request regarding the electrical testing on site.

465 Regarding the no-fire test, the document of actuators' requirements (Ref. 65) does not specify that the apparent two different tests, no-fire and all-fire, are in reality two steps of a same unique destructive test.

466 The sensitive aspect of any initiator is an electric current to the bridgewire. If the value of the electrical current is sufficient, but lower than the no-fire value, electrical properties of the bridgewire may vary out of the range of no-fire/all-fire requirements, which may then impact on the safety requirements. The no-fire characteristic of initiators is not limited solely to the no-fire test. It is linked to the EICs' specification: 300s after the RELEASE event, EICs must not be able to deliver a current higher than the no-fire value. This means that there is a scenario when an initiator might receive a current, which may impact the bridgewire properties, subsequently affecting the design intent of the initiator. This scenario could be initiated as a result of a C&I fault.

467 Such a scenario could occur in the case of C&I failure. An intermittent failure within the C&I could also lead to a repeat of this scenario.

468 In summary, I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall provide the justification that C&I faults do not impact the properties of the initiator bridgewire.

4.10.2.5.13 Relevance to UK

469 Westinghouse used many US documents to design cartridges and EICs. Notably, the qualification plan for actuators (Ref. 89) of the EMI test procedure (Ref. 90) refers to US standards and guidance. In addition, the cartridge management requires phases of transportation, testing, and storage within the Nuclear Power Plant.

470 Some of the items mentioned above may be covered by relevant British (or European) Regulations and standards. Thus applying US standards or guidance may not be adequate in the UK.

471 I have questioned Westinghouse regarding associated relevance to the UK TQ-AP1000-703, (Ref. 10). Westinghouse responded that the Codes and Standards Report will be issued in December 2010. However, Westinghouse then stated that the relevance of US standards and guidance used for squib valve designs would be captured in a dedicated report.

472 I consider this to be part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate and issue the justification that all the relevant UK requirements for the design of cartridges and EICs, have been adequately covered by the implementation of US standards and guidance.

4.10.2.6 General Surveillance and EMIT

4.10.2.6.1 Tasks and Periodicities

473 I judge the important safety role of the squib valves, and the inability to stroke the valves as an inherent characteristic of the designs, drive the surveillance and EMIT regime to be a significant consideration in assessment of the squib valve concept as part of the AP1000 nuclear power plant design.

474 An ND internal peer review has endorsed this position, which is derived from the fact that the squib valve design does not allow it to be stroked on a periodic basis, due to the design incorporating a number of sacrificial components when actuated. I consider it is a normal EMIT requirement for a safety important valve to be stroked periodically.

475 In September 2010 Westinghouse explained in detail their planned surveillance and EMIT regime for the squib valves (Ref. 68), which I have used as the basis for my assessment. I noted from the explanations that:

- All valve bonnet flanged bolting is to be inspected and checked for tightness during each refuelling outage.
- In accordance with ASME OM code, ISTC 5260 (Ref.49), 20% of cartridge assemblies for each valve type are to be replaced, with the old cartridges being fired during each refuelling outage.
- In accordance with ASME B&PV Code, Section XI, division 1 Table IWB 2500-1 Exam Cat B-G-1, item B6.2120, each valve shall be removed from its system to allow

the flange faces to be visually inspected, every 3 years or the subsequent scheduled refuelling outage (IWB-2500-12).

- In accordance with ASME B&PV code, Section XI Div 1 Table IWB 2500-1, Exam Cat B-P item B15.70, each shear cap to be leak tested (IWB-5520), each refuelling outage.
- An NDT inspection is to be carried out on one shear cap of each design every 10 years.
- An NDT inspection is to be carried out on one tension bolt of each design every 10 years.
- In accordance with ASME B&PV code, Section XI Div 1 Table IWB 2500-1, Exam Cat B-M -2 item B12.50 the valve body internal surfaces are to be visually inspected each time a valve body is dismantled.
- Each valve component is to be visually inspected, each time a valve is dismantled.

476 Discussions confirmed that maintenance system preparation i.e. isolation, line drainage requirements, and valve removal is a significant aspect of the task. Due to the novel design and the limited reliability evidence available to date, I expect a shear cap inspection to be concurrent with the identified inspection of each flange, i.e. every three years or the subsequent scheduled refuelling outage.

477 Westinghouse is also recommending the following EMIT specific to the 8 inch Squib valve:

- In accordance with ASME B&PV code, Section XI Div 1 Table IWB 2500-1, Exam Cat B-G-2 item B7.70 bolts, studs and nuts are to be visually inspected every 3 years or the subsequent refuelling outage.
- The latch spring is to be functionally verified during each refuelling outage.
- Each 8 inch valve is to be visually inspected for leakage through its shear cap during each refuelling outage.
- Each 8 inch valve positional switch is to be functionally verified during each refuelling outage.
- Each 8 inch valve piston position is to be functionally verified during each refuelling outage.

478 Discussions confirmed the verification would likely to be limited to the valves that have the propellant cartridges replaced as it is this aperture that will be utilised to deploy a dedicated tool to carry out the verification. Due to the novel design and the limited reliability evidence available to date, my expectation is that each valve piston position is verified and this check is not limited to the ones that have their cartridge removed. This is Westinghouse's strategy for the 14 inch squib valve (i.e. verify all valve positions), as the verification is carried out via the valve exhaust port and there is no requirement to remove the propellant cartridge to provide the necessary access.

479 In addition, Westinghouse are also recommending the following EMIT activities specific to the 14 inch Squib valve:

- In accordance with ASME B&PV code, Section XI Div 1 Table IWB 2500-1, Exam Cat B-G-1 item B6.210 bolts, studs and nuts are to be visually inspected every 3 years or the subsequent refuelling outage.

- Each 14 inch shear cap clamp is to be visually inspected and torqued during each refuelling outage.
- Each 14 inch shear cap retainers are to be inspected and torqued during each refuelling outage.
- Each 14 inch support ring is to be inspected and torqued during each refuelling outage.
- Each 14 inch piston position is to be verified during each refuelling outage.
- Each 14 inch positional indication is to be functionally verified during each refuelling outage.

480 However, given the safety importance of the squib valve designs, and the required 60 year design life, I consider that Westinghouse should justify why it is not considered prudent, and reasonably practicable, to periodically test the sacrificial items of the squib valve types (in a separate valve body designated for this purpose) in order to maintain confidence that the valve will operate successfully on demand.

481 TQ-AP1000-1094 (Ref. 10) response describes Westinghouse's consideration and ALARP justification that the surveillance and EMIT proposed is adequate. Whilst I generally accept their ALARP justification for not carrying out a whole actuation test, I attach great importance to the implementation of an adequate surveillance and EMIT regime.

482 Westinghouse subsequently issued the Squib Valve Surveillance and EMIT report formally (Ref. 68), which I consider does not give adequate consideration to my expectations discussed at the September 2010 technical meeting. Westinghouse agreed to review and update the report against my expectations, prior to its formal issue and my detailed assessment. Westinghouse's previous explanation of the proposed surveillance and EMIT requirements clearly identified the requirements to remove each squib valve from its system on a periodicity of 3 years, or if then at power, the subsequent outage. However, this is not reflected in this latest documentation (Ref. 68). The lack of consideration to my expectations is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate evidence of recommending an adequate surveillance and EMIT regime that is commensurate to the AP1000 NPP safety case assumptions and the safety role of each squib valve type.

4.10.2.6.2 EMIT Enabling Activities

483 My assessment of the maintenance studies and the sequential enabling activities involved in the removal of each of the squib valves from their associated system pipework has concluded:

- The maintenance study is at an early stage, and there is evidence that new DCPs will be required to support the removal of squib valves from the system pipework, for example:
 - i) A jib crane is required to be transported into the containment and attached to the room wall each time a 14 inch ADS squib valve is manoeuvred.
- Each injection squib valve is physically mounted directly above a recirculation squib valve. This introduces the requirement to remove an injection squib valve to provide access to a recirculation squib valve, which confirms that space is limited in these areas.

- It is unclear what provision there is within the overall AP1000 design to aid the assembly of the jib and supporting services. Assessment of other topic areas has identified that space is limited and it is necessary that the whole design complies with all relevant UK health and safety legislation, which is part of squib valve GDA Issue (**GI-AP1000-ME-01**).
- It is proposed to maintain the squib valves in a dedicated area within containment although it is possible to transport the squib valves out of the containment area and carry out any necessary maintenance in the hot workshop. Manoeuvring the valve requires the support of a bogie to transport the valve between the room location and the floor access hatch, which in principle is considered acceptable.
- The system designs do not appear to incorporate adequate arrangements to aid the depressurisation or the draining of the system pipework prior to removing a number of squib valves from the system pipework, which is part of GDA Issue (**GI-AP1000-ME-03**) Mechanical System Pipework Design.
- There is evidence that mechanical sequence diagrams are being generated to aid the understanding of EMIT activities, which can also be utilised to aid peer and system reviews, which is in line with my expectations.

484 Westinghouse used evidence from the 3D model to confirm that no items important to safety are located in the vicinity of the exhaust path of an actuated 4th stage squib valve. The model shows that the exhaust path for the coolant is against a plain wall, at an elevation that is above the height of the personnel access door to the room.

485 My assessment has confirmed the 3D model is considered as a visualisation tool, rather than a quality controlled design tool and record. I expect the maintainability studies to take due recognition of this.

486 In summary, from a GDA and a Mechanical Engineering perspective I am now satisfied that Westinghouse is carrying out an adequate spatial, ingress and egress review for carrying out the replacement activities for the squib valves.

487 Westinghouse has clarified in TQ-AP1000-1102 (Ref.10) response that all four ADS 4th stage squib valves require be operable during modes 1 to 4. During modes 5 and 6 either one or 2 squibs valves may be taken out of service and removed in support of carrying out EMIT requirements, which is to be controlled by a Operational Technical Specification. System isolation is achieved via the closure of a dedicated motor operated isolation valve. However, I noted the system design then leaves a dead leg downstream of the 14 inch ADS squib valves, which can only be drained via add hoc means i.e. splitting of flanges and use of temporary fluid collection containers.

488 My assessment has identified:

- The injection squib valves are isolated from the IRWST via a single isolation valve and the Reactor Coolant System is isolated via freezing the pipework in a convenient position.
- The recirculation squib valves are also isolated from the IRWST by freezing the pipework in a convenient position.

489 Westinghouse's arguments for selecting the freezing technique are based on:

- The squib valves only require to be removed from the system pipework on a limited number of occasions during the life of the operating plant.
- Minimising the number of valves on the reactor coolant primary circuit pipework.

- 490 I consider (from earlier discussion concerning the EMIT and surveillance requirements for the squib valves) there are now an increased number of occasions when each squib valve is required to be removed from its associated system pipework. I also consider the second argument not be consistent as each 4th stage ADS squib valve is isolated via a motor operated valve within a branch off the primary reactor coolant pipework (Figure 4).
- 491 The design incorporates a single isolation valve to contain the IRSWT. Westinghouse considers this to be acceptable due to the fluid temperature being less than 200°C, and the process line being at nominally atmospheric pressure. However, the IRWST contains circa 2100m³ of fluid and if the single isolation valve was to fail then a significant flooding hazard would arise. The system design does not have any other provision to contain the fluid within the IRWST.
- 492 The draining of the line between the reactor coolant primary pipework and the squib valve is again by ad hoc means i.e. splitting of flanges and use of temporary fluid collection containers.
- 493 My assessment has now identified that Westinghouse has updated the applicable system designs to incorporate draining arrangements for all other aspects of the squib valves via design a change (Ref. 55), which is now approved for implementation. The revised arrangements are shown on updated design documentation (Ref. 56).
- 494 These arrangements typically consist of a small bore branch line, which is located local to a squib valve. The branch line incorporates an isolation valve and plug to provide an isolation role (containment safety function) during normal operations. To support the system draining requirements the plug is removed, which allows the system fluid to be collected locally in a suitable container and subsequently processed. The exception to this is the system pipework that is located between the recirculation squib valves and the sumps. These system lines drain by gravity into their associated sump, noting that the two check valve discs are manually repositioned with the aid of a special tool.
- 495 Given the surveillance and EMIT requirements that are now associated with the squib valves, the time the system relies on a single valve for isolation (containment safety function) has increased. In addition the prerequisite to the removal of a recirculation squib valve is the removal of an injection squib valve due to spatial constraints. This is an integral part of the GDA Issue (**GI-AP1000-ME-03**) that I have raised on the topic of Mechanical System Pipework Design.

4.10.2.7 Regulatory Observation Responses

- 496 Westinghouse has identified the listed documents in support of closing out the ten squib valve Regulatory Observation Actions, which are tabulated below.

RO-AP1000-036 Deliverables

Item	Description	Westinghouse Ref. No.
1	Squib Valve Functional Test Sensitivity Analysis Engineering Test analysis. (which is presented as an appendix within the Prototype Test Report).	Prototype Test Report 10.4.368 Rev 0 (Ref. 70) Appendix B

Item	Description	Westinghouse Ref. No.
2	Design Specification: Squib (pyrotechnic actuated) Valves, ASME Boiler and Pressure Vessel Code, Section III Class1.	APP-PV70-Z0-001 Rev G (Ref. 57)
3	Design Specification: Pyrotechnic Actuator for ASME Boiler and Pressure Vessel Code, Section III Class1 Squib Valve (PV70).	APP-PV98-Z0-001 Rev 0 (Ref. 65)
4	Prototype Test Report	10.4.368 Rev 0 (Ref. 70)
5	Squib (pyrotechnic actuated) Valves, In-service Testing Recommendations.	APP-PV70-VM-001 Rev 0 (Ref. 68)
6	AP1000 Squib Valve Failure Modes and Effects Analysis FMEA.	APP-PV70 GRA-001 Rev 0 (Ref. 45)
7	ASME Class 1 code Report.	10.2.189 Rev 0 (Ref. 62) 10.2.190 Rev 0 (Ref. 63) 10.2.191 Rev 0 (Ref. 64)
8	Equipment Qualification reports	To be advised
9	Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary.	APP-PV70-GER-002 Rev B (Ref. 61) APP-PV70-GER-002 Rev 0 (Ref. 69)
10	Development Report Squib Valve Ballistics	To be advised

497 I consider the identified deliverables are required to be formally approved and issued once they reflect the squib valve final designs. This will then allow formal assessment to be undertaken and progress made in formally closing out the squib Valve GDA Issue.

498 During Step 4 Westinghouse has described their summary report (Ref. 69), which on completion is to provide the auditable narrative of the squib valve design from initial conception to the final design. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall finalise the Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary Report that represents each squib valve final design.

499 Westinghouse has now issued the Test Report (Ref. 70), which describes the:

- Development tests undertaken to confirm the concept principle, and its functionality.
- Increased understanding of the valve characteristics during an actuation.
- Evaluated test data.
- Development of the design, while undertaking the prototype tests.

500 I consider the Test Report (Ref. 70) provides a good audit trail and provides the general arguments to the development reasoning of the valve design, from its original principles to its current design status.

501 Westinghouse has also issued reports (Ref. 62, 63, & 64) that describe and provide evidence as to how the valve design has been considered against the ASME Boiler and

Pressure Vessel Code requirements. The reports are generally in accordance with my expectations, although I do note:

- The analysis has not been carried out to the current ASME edition. I discuss this aspect further under the Codes and Standards topic.
- The ASME class code reports (Ref. 62, 63, & 64) contain open items, and hence may be the subject of a future update. I therefore consider this to be part of the Squib Valve GDA Issue; Westinghouse to provide formally approved design substantiation in support of the squib valve final design.

502 My assessment of the FMEA was conducted against a risk assessment methodology (Ref. 45) that is in line with my expectations. The FMEA identified the design characteristics, potential failures, human errors associated with operating and carrying out maintenance of the valve, the aspects that needed to be considered important to safety, the hazards and risks that were required to be fully understood, and were either mitigated or adequate measures put into place to manage them.

503 Westinghouse has not followed my earlier regulatory guidance to include an independent representative at future FMEA reviews. This is part of the Squib Valve GDA Issue (**GI-AP1000-ME-01**); Westinghouse shall generate evidence that the FMEA for the final squib valve designs includes evidence of independent technical review.

4.10.2.8 Squib Valve Assessment Summary

504 In summary, I consider my Step 4 assessment of the squib valve topic has made meaningful progress, and I have gained a sufficient level of confidence in some areas to limit future assessment requirements. However, throughout undertaking my Step 4 assessment, the designs have continually evolved, which has limited availability of formal documentation representing the final designs for assessment. Given the importance of the squib valve concept within the safety justification for the AP1000 design, and the novelty of the design in terms of NPP application, I am not yet satisfied from a GDA Mechanical Engineering perspective. I therefore consider the squib valve topic to be a GDA Issue (**GI-AP1000-ME-01**).

4.10.3 Findings

GI-AP1000-ME-01: *Given the development status of the squib valve designs, the importance of the squib valve applications within the safety justification for the AP1000 design, and the novelty of the design in terms of NPP application, I am not yet satisfied from a GDA Mechanical Engineering perspective. I therefore consider the squib valve topic to be a GDA Issue.*

505 To resolve this GDA Issue, Westinghouse shall:

- Generate and issue appropriate approved documentation that provides adequate arguments and evidence for the squib valve selection, equipment design, and associated system designs, or satisfy the expectation by alternative means agreed by the Regulator.
- Generate and issue sufficient documentation to justify the squib valve detailed component design is able to achieve the safety case requirements and assumptions or satisfy the expectation by alternative means agreed by the Regulator.

- Provide sufficient documentation to justify that the squib valve interfacing system designs (e.g. supports, interfacing pipework etc.) are able to achieve the safety case requirements and assumptions, or satisfy the expectation by alternative means agreed by the Regulator.
- Provide sufficient documentation to demonstrate the surveillance and EMIT regime is able to achieve the safety case requirements and assumptions. Given the 60 year design life of the AP1000, and inability to stroke the squib valves during in service inspections, I consider that Westinghouse needs to provide a robust surveillance regime to ensure that the squib valve designs are capable of delivering their safety functions in accordance with the requirements of the safety case, or satisfy the expectation by alternative means agreed by the Regulator.

4.11 Safety Relief Valves

506 I undertook an assessment of the AP1000 safety relief valve arrangements during my Step 3 assessment, and did not identify any concerns with this equipment (TQ-AP1000-181, 182, 183, Ref. 10). I followed up this topic area during Step 4, through discussion at a technical meeting with Westinghouse in Pittsburgh, and I also raised assessment questions regarding the Power Operated Relief Valves (PORVs) used on the steam generation secondary side, used to control pressure through steam relief.

507 During my Step 3 assessment activity, Westinghouse had also made reference to their Over Pressure Protection Report as evidence to substantiate their design, and process, in terms of over pressure protection for both the primary circuit and the secondary side circuit. I decided to review this document as an example of evidence during Step 4. During Step 4 I also decided to review the Low Temperature Overpressure Protection (LTOP) provisions within the AP1000 design, due to the vulnerability of primary circuit materials at low temperatures, due to their lower mechanical toughness under these conditions.

508 I consider the following Safety Assessment Principles to be relevant to these aspects:

- Safety Assessment Principle EPS.3 (Ref. 4) states 'Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.'
- Safety Assessment Principle EPS.4 (Ref. 4) states 'Overpressure protection should be consistent with any pressure-temperature limits of operation'.

4.11.1 Assessment

4.11.1.1 Safety Relief Valve Designs

509 Westinghouse described the pressuriser safety relief valve, the main steam safety valves, and the normal residual heat removal system pump suction relief valve, following the responses to the associated technical queries.

510 Westinghouse claimed that they had experienced no significant adverse feedback in respect of their safety relief valve designs, TQ-AP1000-181, 182, 183 (Ref. 10).

511 The valves are procured to QME-1-2007, and the EMIT recommendations to the utilities will be in line with the ASME requirements.

4.11.1.1.1 Pressuriser Safety Relief Valves

- 512 The Pressuriser Safety Relief Valves provide a containment safety function, by limiting the pressure within the primary circuit, and directing any fluid discharge through a defined route, as well as providing a containment function under normal operation within system design pressures. They are a standard feature of a Nuclear Power Plant.
- 513 The AP1000 Pressuriser Safety Relief Valves have the following design and technical characteristics:
- Two valves are located on top of the pressuriser.
 - These are 'pop type' (rapid opening) direct loaded spring relief valves.
 - They incorporate a qualified position indication device that can be monitored in the control room.
 - The valves are designed to ASME Code Section III, Sub-section NB (Class 1).
 - Tests before installation cover hydrotest, seat leakage, and set pressure. The vendor would undertake the tests, based on instruction and witnessing by Westinghouse and the utilities as necessary.
 - Testing before power generation covers verification of set pressure.
 - The design life of the valve is 60 years, although this requires a degree of refurbishment.
 - The same pressuriser safety relief valve design configuration is used on existing Westinghouse PWRs.
- 514 Westinghouse reported OEF relating to seat leakage, attributed to the system being pressurised too quickly, and set point drift discovered during offsite testing (although the valves were still operating within their design conditions). Westinghouse stated that the valve test regime is designed to control and reduce these adverse characteristics, and any set point drift would remain within the design tolerance.

4.11.1.1.2 Main Steam Safety Valves

- 515 The Main Steam Safety Valves provide a containment safety function, by limiting the pressure within the secondary side steam circuit, and directing any fluid discharge through a defined route, as well as providing a containment function under normal operation within system design pressures. They are a standard feature of a Nuclear Power Plant.
- 516 The Main Steam Safety Valves have the following design and technical characteristics:
- They are 'pop type', direct loaded spring relief valves.
 - A total of six valves are provided per Steam Generator, designed to open at slightly increasing set pressure values.
 - The valves are designed to ASME Code Section III, Sub-section NC (Class 2).

- Position indication is provided which can be monitored in the control room.
- Tests before installation cover hydrotest, seat leakage, and set pressure.
- Testing before power generation covers verification of set pressure.
- The same design configuration has been used on existing Westinghouse PWRs.

517 Westinghouse stated that an Institute of Nuclear Power Operators (INPO) search identified issues with pilot operated valves, but the Westinghouse valves are not of this type. The issues identified from OEF relate to seat leakage and set point drift, which Westinghouse stated were controlled through the testing regime.

518 Westinghouse stated that the revised overpressure protection report addresses the capacity requirements for these safety relief valves.

4.11.1.1.3 RNS Safety Relief Valve

519 The RNS Safety Relief Valves provide a containment safety function, by limiting the pressure within the Normal Residual Heat Removal (RNS) circuit, and directing any fluid discharge through a defined route, as well as providing a containment function under normal operation within system design pressures.

520 The RNS Pump Suction Relief Valve has the following design and technical characteristics:

- The valve is a direct loaded spring relief design, which is of the gradually opening type (as opposed to the 'pop type').
- The valves are designed to ASME Code Section III, Sub-section NC (Class 2).
- Tests before installation cover hydrotest, seat leakage, and set pressure.
- No testing before power generation is required.
- The same RNS relief valve design configuration has been used on existing Westinghouse PWRs.

521 Westinghouse stated that past operating experience has demonstrated that this valve type is adequate for the intended application. No adverse incidents have been reported on the INPO database based on a search of the past five years. Typical issues with this valve design are seat leakage and set point drift, which are controlled by the test regime.

4.11.1.1.4 Power Operated Relief Valve

522 The Power Operated Relief Valves are control valves used within the secondary side steam circuit of the AP1000. In conjunction with the Main Steam Safety Valves, they provide over pressure protection for the secondary side circuit.

523 Westinghouse provided information on the Power Operated Relief Valve (PORV) used on the steam generation secondary side circuit (TQ-AP1000-1261, Ref. 10). They commented that no PORV had been provided in the pressuriser due to the simplification philosophy associated with the AP1000 design.

- 524 The PORV has the following functions within the AP1000 design, namely overpressure protection, atmospheric steam dump, and safety isolation.
- Overpressure protection – the PORVs prevent unnecessary actuation of the Main Steam Safety Valves. The PORVs incorporate an operator defined pressure controlled setpoint, which is less than the lowest MSSV set pressure. The PORVs also allow for smooth and reliable re-seating of the Main Steam Safety Valve (MSSVs).
 - Atmospheric Steam Dump – the PORVs provide a diverse cooldown method, and they prevent unnecessary activation of the PRHR HX. In respect of public and personnel design considerations, a silencer is used to reduce ambient noise.
 - Safety Isolation – PORVs are steam-line and steam generator isolation valves, but are not isolation valves for the containment building; this function is provided by the block valves located up stream. The PORVs are air operated valves using solenoid pilot valves which port air pressure to effect a valve closure.
- 525 The PORV safety functional requirements are summarised as follows:
- Failure of a single power supply will not result in a failed PORV and PORV block valve.
 - The PORV should not fail open on loss of power.
- 526 The PORV has the following technical characteristics:
- The PORV diaphragm materials provide good tolerance to radiation and temperature effects.
 - PORV seat leakage detection and mitigation is provided.
 - A safety classified PORV pneumatic supply is provided in respect of leakage and maintenance.
- 527 The PORV utilises a globe valve design, and the design is fitted with hand wheels such that manual control is available without instrument air being available. Westinghouse commented that they were reviewing the physical positioning of this wheel to make operation convenient and ensure it was practicable. The physical operation of the valve uses a piston type arrangement where compressed air is ported to the spaces above and below the piston head; noting that a spring is also provided to automatically close the valve on loss of pressure.
- 528 Westinghouse described their company QA surveillance regime associated with the manufacturing process, and described the witness hold points used to verify the manufacturing process. They explained that the detail of this requirement would be determined following receipt of the supplier's quality and manufacturing plan, which they will approve. They stated that more oversight would be applied to suppliers who are new to Westinghouse.
- 529 Westinghouse described the maintenance arrangements associated with the PORVs, noting they envisaged a 60 year life with normal maintenance. The specific maintenance requirements will be developed in liaison with the supplier.
- 530 They described the operational experience associated with PORVs, noting that their design is consistent with in-service valve designs, and this design reflects 40 total years and over 1000 reactor years of experience. Operating experience has also been captured from external sources, including INPO, US NRC, Customer Feedback, and Manufacturers and Suppliers.
-

4.11.1.1.5 Safety Relief Valve Summary

531 In summary, I am satisfied with the design specifications described for the safety relief valves for the AP1000 design. I consider that they represent mature designs, with an established pedigree, and I have not identified any areas for concern through undertaking my assessment against SAP EPS.3.

4.11.1.2 Over Pressure Protection Report

532 I continued my assessment in respect of the Over Pressure Protection Report provided during Step 3.

533 During a Step 4 technical meeting I provided a background to this regulatory line of enquiry (over pressure protection); namely that this document had been provided in response to a technical query, but that my review of the document had found the explanation (narrative) difficult to follow, and cross references to the relevant sections of the ASME code had not identified a clear and transparent mapping to the code requirements.

534 Westinghouse stated that a separate, internal QA review of this document had identified effectively the same issues. Although the report is consistent in format to that produced for other designs, Westinghouse has independently decided that the report should be much clearer in format and content.

535 I stated my expectation that this document should be clearer, tell a better narrative, and identify a clearer mapping to the requirements of the applicable code. This should be undertaken in sufficient time to meet the Step 4 assessment timeframe requirements, and Westinghouse agreed to progress.

536 At a subsequent technical meeting Westinghouse described the recent revision to the Over Pressure Protection Report (Ref. 72), in response to the mechanical assessment line of enquiry. Westinghouse stated that internal assessment of the report has resulted in a complete revision to the document, and the revised document now fully complies with the requirements of Article NB-7000 of Section III of the ASME Code.

537 I have reviewed this revised document, which I consider to be a significant improvement on the previous version, and which presents a far more coherent, rational, and understandable explanation and justification. I have also observed that the document had been sealed by an American Professional Engineer.

538 My intervention in this area has been largely driven by the expectation that Westinghouse should present a good quality document to meet the requirements of the ASME code, in accordance with their stated design approach and safety claims. I am now satisfied with the progress made in this respect, and the clarity of information within the revised document against SAP EPS.3.

4.11.1.3 Low Temperature Overpressure Protection

539 I asked Westinghouse to describe the Low Temperature Overpressure Protection System (LTOPS) associated with the primary circuit, due to the greater susceptibility of primary circuit material to mechanical failure at low temperature, (TQ-AP1000-1132, Ref. 10).

540 In response to this line of enquiry, Westinghouse provided document 'AP1000 LTOPS Analysis / Normal RNS Relief Valve Sizing Evaluation', (Ref. 77).

- 541 The low temperature overpressure protection is provided by either of the inside containment relief valves on each of the two RCS to RNS pump suction lines of the Normal Residual Heat Removal System. Although both of the RCS to RNS pump suction lines are aligned for normal plant cooldown, the alignment of either one of the two trains provides full protection.
- 542 The relief valve sizing evaluation (Ref. 77) has addressed protection of the primary circuit materials, based on a limiting temperature of 275 degrees F (135 degrees C), which is the LTOPs arming / enable temperature (i.e. the LTOPs must be operable below this temperature). The sizing evaluation contains four open items, since some of the parameters used in the calculation were not finalised at the time of production of the report. Westinghouse has stated that upon finalisation of these values, the report will be reviewed and the open items closed; which I consider to be an Assessment Finding (**AF-AP1000-ME-15**).
- 543 I also note that a number of parameters associated with the LTOPs require translation into plant limits and conditions (Operating Rules), which is identified in the Westinghouse response, and which I consider to be part of normal process.
- 544 Notwithstanding the Assessment Finding, I am satisfied with the design description and explanation from a GDA perspective against SAP EPS.4.

4.11.2 Findings

AF-AP1000-ME-15: *The sizing evaluation for the LTOPs contains four open items, since some of the parameters used in the calculation were not finalised at the time of production of the report. The licensee shall ensure that the LTOPs justification has been completed and all open items have been satisfactorily closed out. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.12 Reactor Coolant System Pump

- 545 I consider the role of the reactor coolant pumps (RCP) to be important to safety.
- Safety Assessment Principle ECS.1 (Ref. 4) states 'The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety'.
 - Safety Assessment Principle EMT.1 (Ref. 4) states 'Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.'
 - Safety Assessment Principle EQU.1 states (Ref. 4) 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'
- 546 I have specifically focussed my assessment on the Mechanical Engineering features of the RCP that manage the following primary safety functions:
- Heat transfer and removal.
- 547 As Westinghouse introduced a design change at the start of Step 4, which introduced a different pump design for the UK, my assessment has further targeted the:

- RCP design.
- Pump safety classification.
- RCP EMIT and replacement.
- Flywheel verification.

4.12.1 Assessment

4.12.1.1 RCP Design

548 At the start of the Step 4 process Westinghouse advised that the AP1000 design for the UK is to progress utilising a KSB type pump (KSB is a European manufacturer). Westinghouse stated the change will be implemented by following their design change process.

549 The design change was initiated at the request of the potential UK future licensees who preferred the use of a wet winding pump on the grounds of improvements in operational efficiency. Westinghouse has confirmed that the AP1000 design for their home US market is to retain the EMD pump design (EMD is a US manufacturer), which has NRC certification.

The KSB pump is a seal-less design type, designed to meet applicable sections from relevant US and European nuclear codes and standards, operating at a frequency of 60 Hz as spatial constraints prevents a 50 Hz pump from being installed. The system is required to include suitable electrical equipment to align the frequency to the UK standard of 50 Hz.

550 There are significant differences between the EMD pump planned for the US and the general world market, and the KSB pump which is specified for the UK AP1000 design. In particular, the KSB pump has the following different technical characteristics:

- it is of a single flywheel design;
- it is of an integrated wet winding motor design;
- it includes an additional bearing;
- it is of a forged flywheel design with a hirth type fixing connection;
- it is of a metric design, except for the mating RCS interface flange;
- it is a concept / development design (at the time of GDA);
- it has an undefined maintenance strategy.

551 My initial discussions regarding this new pump have clarified:

- The proposed pump design is a new design of pump for KSB, noting the concept has evolved using KSB proven principles and the utilisation of proven features from two existing pump designs.
- KSB has experience of both wet and dry winding pump designs.
- KSB has constructed and tested a half scale pump with the results being aligned with an associated analytical study.
- The Westinghouse strategy for demonstrating functionality and safety functional requirements is via the Factory Acceptance Tests on the construction of the first production pump.

- 552 KSB is an established organisation with a manufacturing and servicing presence across all the world continents in the provision of pumps for a wide range of industries, which includes the nuclear power generation industry, and has grown since the organisation was originally set up back in 1871.
- 553 They have been involved in wet winding pump designs and technology since 1953. Their design strategy is driven from a commercial aspect as a wet winding design offers a potential saving of 8% in energy consumption, when compared to a dry windings design.
- To date KSB has followed their normal design process for the development of the proposed type of pump, with the pump engineering principles, hydraulics and calibration being substantiated at scale, with further qualification only being carried out on each production pump.
- 554 Westinghouse plan to treat the proposed RCP for the UK AP1000 as a First Of A Kind (FOAK) pump and it will be tested in accordance with the AP1000 Design Specification (Ref. 21), which will include fitting the pump unit into a dedicated test loop. Examples of the tests that will be carried out for a FOAK unit include, (but not limited to):
- 500 hours operational test against the entire range of expected flow rates and speeds to verify the hydraulic performance.
 - Transients that have been agreed between the supplier and the purchaser.
 - Demonstration that the flywheel will perform as designed, including a 125% overspeed test and a visual inspection.
- 555 Subsequent production pumps will be tested in accordance with the AP1000 Design Specification (Ref. 21), which also includes fitting the pump unit into a dedicated test loop. Examples of tests carried out on a production unit include, (but not limited to):
- 50 hours operational test against plant conditions.
 - Transients that have been agreed between the supplier and the purchaser.
 - Demonstration that the flywheel will perform as designed, which includes a 125% overspeed test, which is followed by a visual inspection.
- 556 The design concept for the AP1000 is considered complete along with the pump design substantiation. As a supplier, KSB are in position to proceed to the manufacturing phase of a production pump. However, Westinghouse under their design process require to undertake their final design review of the pump, which is to be carried out in two phases, one prior to manufacture and testing, with the second post test to take into account feedback (from the test).
- 557 The pump design incorporates vibration monitoring equipment with the function of monitoring the balance status of the pump. I consider the vibration monitoring system to be important to safety, as it provides an indication of the balance of the shaft, which is attached to the flywheel that has a safety function to provide adequate coast down momentum to ensure sufficient transfer of heat from the reactor in a fault scenario. The response to TQ-AP1000-688 (Ref. 10) and the revised safety classification document (Ref. 35) provide evidence that the vibration monitoring equipment is assigned with a safety categorisation of C and a classification 3, which is aligned with my expectation.
- 558 Westinghouse claim that the design criteria for the pump is a sixty year design life, and with no maintenance. However, it became apparent from discussions with KSB that their experience is leading to the recommendation of carrying out a preventative maintenance regime by inspection of the following aspects during certain scheduled shutdowns:

- Thrust bearings.
- Lower radial guide bearing.
- Cable penetrations.
- Winding insulation.

559 I noted from discussion that the seals have a design life of 60 years. However, I was unclear if the seal at the pressure boundary that feeds the windings has been assessed for the impact of radiation ageing. I consider this to be an Assessment Finding (**AF-AP1000-ME-16**); a future licensee to generate evidence that the pump seals have adequately considered the effect of radiation ageing for a 60 year design life.

560 The response to an Intermediate Design Review action (Ref. 20) provides the evidence that the pump design has considered the impact of crud particles (solids within the primary circuit), with consideration to operating experience and has incorporated a number of design features to manage these potential crud particles. These features include:

- A crud trap is positioned below the impellor, where particles that have passed the two gaps between the back shroud and impeller hub are collected.
- A second trap collects particles from between the impeller and the diffuser that have not travelled past the gap at the back shroud.
- A third trap, collects particles from around the flywheel. The design collects particles at the lower end of the outside diameter of the flywheel cavity.
- A fourth and final trap collects particles from the area below the thrust bearing tilting pads, which is the lowest spot where remaining particles can lie within the pump design.

561 The pump bearing design arrangement consists of two radial guide bearings positioned within the motor section, a further radial guide bearing positioned between the flywheel and the impellor and a double acting thrust bearing that is positioned at the lower end of the motor. The bearing material is Carbon Reinforced Fibre and the half scale model test provided evidence of the design achieving its design intent.

562 The test subjected the bearings to approximately [REDACTED] start-stop sequences; (operational design requirements over a 60 year operation of an NPP is in the region of 1000 start-stop sequences). During normal steady state operation the bearing does not encounter any wear, as it is hydrodynamic in operation.

563 An intermediate inspection undertaken following approximately [REDACTED] stop-start sequences identified visible signs of operation, and the total wear was recorded on the pads and plates as [REDACTED]. A final inspection was undertaken following approximately [REDACTED] stop-start sequences, which also confirmed the bearings remained within the design tolerance limits, with the total wear being recorded as below [REDACTED].

564 I consider the results provided evidence that the bearings are capable of achieving their 60 year design life without the requirement to replace them.

565 Westinghouse has explained that a design change was implemented during the development of the AP600 nuclear power plant design to specify the Reactor Coolant Pump to be of a single standard design. This proposal allows for each pump to be interchangeable within a single plant and limits the number of strategic spare pumps for a

plant. However, this means that as the pumps now have the same rotational direction, then asymmetry is introduced into the fluid flow regime within the primary circuit.

566 My assessment of the Reactor Coolant Design Specification (Ref. 21) confirms the inclusion of this design constraint.

567 I was satisfied with this explanation, although this asymmetry has had derivative implication in terms of performance of the fluid within the RCS, in the event of inadvertent actuation of the PHRR HX. This aspect is discussed elsewhere in this report.

4.12.1.2 RCP Safety Functions and Classification

568 Following assessment of EDCD Chapter 5 (Ref. 88), I consider the pump has duty safety functions, which are to support the transfer of heat within the primary coolant system under power operations, and normal decay heat removal conditions, and to provide a pressure boundary containment safety function. Furthermore, the pump has a safety function under fault scenarios of providing an adequate coast down performance for heat transfer. My Mechanical Engineering assessment has taken due regard of these safety functions. I acknowledge that evidence of the pump and the integrated system achieving their safety functions is provided by undertaking the FATs and SATs, including the system integrated tests.

569 I have now identified that the pump has been assigned with a Category A safety function for maintaining the reactor coolant system pressure boundary, and for pump coast down performance, with associated parts assigned as Classification 1, from my review of the updated safety categorisation and classification document (Ref. 35). This is now generally aligned with my expectations.

570 From a Mechanical Engineering point of view I consider the current concept design specification (Ref. 21) provides a satisfactorily level of evidence that the design parameters for the pump are adequately described for GDA. This document also provides the interface between the Responsible Designer and the pump supplier, who will be responsible for the detailed design and supply of the manufactured item. However, Westinghouse has confirmed the KSB RCP is to have its own dedicated Design Specification, which is in preparation. I consider this to be an Assessment Finding (**AF-AP1000-ME-17**); a future licensee shall generate the formal approved copy of the applicable Design Specification for possible confirmatory assessment.

4.12.1.3 RCP EMIT & Replacement

571 My assessment has determined that if the proposed pump is required to be removed from its installed room to enable EMIT to be carried out, then a temporary facility is required to be constructed. The AP1000 hot workshop is not of a design that can handle the pump and KSB have no facilities to maintain the proposed pump.

572 In response to questions concerning the design taking into account the KSB supplier preventative maintenance requirements, Westinghouse has stated that these aspects are outside the current design scope and they only plan to address these aspects once in contract for an AP1000 unit that is fitted with KSB pumps. I consider this aspect to be an Assessment Finding (**AF-AP1000-ME-18**); a future licensee to develop an EMIT strategy for the AP1000 RCPs, with due consideration to the manufacturer's recommendations for preventative maintenance. I consider that this is a reasonable engineering approach.

573 Westinghouse has described their updated installation sequence of a RCP; they advised that they are only pursuing an understanding of the installation and removal sequence of

the EMD pump design. Their justification for this strategy is that the EMD pump has the bounding volume space envelope and mass.

574 The reduction in mass associated with the KSB Pump, which is in the order of 22 000Kg (33%) between the two pumps, is generally associated with the manufacturing process and use of forging in preference to casting technology.

575 I consider the updated description demonstrated that good progress is being made in understanding the installation sequence of the pump, although spatial constraints remain very challenging to the extent that Westinghouse are proposing to build a full size mock up facility. The facility is to demonstrate the installation sequence for an EMD pump, which will include the fitting of a shield shroud that is required to manage radiation dose uptake during a pump replacement.

576 Discussions identified that a number of physical guides are to be incorporated into the design to aid the installation sequence. This is to facilitate:

- Alignment into the RCS pump bowl.
- Protection against clashing with the steam generators.

577 My assessment has confirmed that the installation sequence and positioning of the Polar Crane as part of the pump replacement sequence is extensively reliant on SQEPs. However Westinghouse has advised they plan for the Polar Crane to be fitted with a number of visual positional indicators. I also note that this is a major refurbishment operation, where the reactor core would be unloaded, and hence the nuclear hazard limited.

578 The description identified the pump room floor is temporarily plated with carbon steel plates, during the installation sequence, to:

- Protect the integrity of the concrete floor, typically from potential dropped loads.
- Provide anchor points to secure and aid winching of the pump installation frame into position.

579 Westinghouse was unable to provide the arguments for the plates being a temporary feature as opposed to a permanent feature, which I consider to be part of an Assessment Finding (**AF-AP1000-ME-19**).

580 The described information did not specifically cover the conventional safety regulations and requirements which are relevant for this type of activity in the UK. I highlighted to Westinghouse that conventional safety regulations are applicable and pertinent to this activity and they are responsible for ensuring the design meets the applicable regulations, e.g. The Construction (Design and Management) Regulations 2007 (CDM), the Lifting Operations and Lifting Equipment Regulations 1998 (LOLER), the Provision and Use of Work Equipment Regulations 1998 (PUWER) etc.

581 My assessment of this topic has included a visit to a local facility where Westinghouse has built a test rig to demonstrate the installation sequence of the EMD pump design. However, the visit did not address my previously raised concerns regarding:

- Spatial constraints in lowering a pump unit between the steam generator and the room walls which are considered to impose risk of damage to other items that are considered important to safety.
- Ability to manoeuvre a pump unit within the room and into a location to raise and fit it adequately within its pump bowl that forms an integral part of the RCS.

- The removal of the existing pump, and the ability to contain, and shield the contaminated aspects.

582 I consider the spatial constraints to be an Assessment Finding (**AF-AP1000-ME-19**); a future licensee is to generate adequate evidence that the AP1000 proposed pump design can be installed and replaced with adequate consideration to UK legislation requirements and without having a negative impact on adjacent SSCs that are considered important to safety.

4.12.1.4 RCP Flywheel Verification

583 From the response to TQ-AP1000-997 (Ref.10) and associated discussions Westinghouse has described their process by which the RCP flywheel coast down requirements are defined and verified at the various stages of the design process and during the plant's operational phase. They confirmed the safety objective of the coast down requirement for each of the RCPs is to ensure a sufficient flow of fluid is achieved following a loss of power scenario to manage the heat transfer from the reactor.

584 The safety analysis requirement is defined within the EDCD Chapter 15 and PCSR Chapter 9. The limiting event is a complete loss of flow, which is classed as a Category II event (classed as a frequent fault for the UK), when there is a requirement to demonstrate no DNB in the core. Westinghouse explained that the design margin is contained within the conservative methodology of the DBA, which defines the coast down requirements that has to be achieved and verified.

585 The design objective is to achieve the required safety coast down requirement, while limiting over sizing of the flywheel, since its inertia generally increases the frictional losses and therefore impacts the operational efficiency of the RCP.

586 The flywheel geometry design was initially targeted to maximise the inertia, while minimising the total mass and stresses within the flywheel. Following the undertaking of a finite element analysis calculation to understand the stress distribution and associated strain displacements, a scaled flywheel test was undertaken, which included the dynamic balancing in 2 planes and an over speed test.

587 Discussions covering this aspect provided the following clarifications:

- The collated empirical test data was aligned with the theoretical data. The theoretical analysis input data took into account the pump head, flow, speed, system pressure, hydraulic efficiency, the geometry of the main parts, and the operating temperatures. Westinghouse considers the alignment of the scaled empirical data with the theoretical data to provide sufficient evidence to enable the flywheel to be scaled up and sized for a full size production pump.
- Chapter 14 of the EDCD (Ref. 88) describes the start-up test procedure for the RCS flow coast-down requirement and for each test a general description is provided with the test objective, prerequisites, and performance criteria where applicable.
- Each RCP flywheel is to be verified during the Factory Acceptance Test phase, prior to its transportation to site.
- The coast-down test is subsequently, only performed during the plant commissioning phase, following initial fuel loading, but prior to initial criticality.

588 It is not transparent within the safety case documentation that the RCP flywheel has been specifically assigned with the appropriate safety classification. I also consider the flywheel coast down requirement to be a safety functional requirement, which requires to

be specified within the safety case and an appropriate Operational Technical Specification. I consider the absence of the RCP flywheel being clearly assigned with a safety classification to be an Assessment Finding (**AF-AP1000-ME-20**); a future licensee to ensure an appropriate safety classification is assigned to the RCP flywheel.

589 Discussion clarified that once a pump has been commissioned there is no further requirement to verify the safety coast down parameters during the operational phase. The response to TQ-AP1000-1221 (Ref. 10) does not provide sufficient arguments or justification for not carrying out periodic verification of the flywheel to demonstrate its ability to achieve its safety functional requirement during the life of a NPP. I consider it necessary that the RCP flywheel coast-down safety functional requirement is periodically verified during the life of an NPP. I consider the topic to be an Assessment Finding (**AF-AP1000-ME-21**); a future licensee to generate their strategy for verifying the safety functional requirement of RCP flywheel coast-down performance during the operational life of their NPP.

4.12.2 Findings

AF-AP1000-ME-16: *The licensee shall generate evidence that the Reactor Coolant Pump seals have adequately considered the effect of radiation ageing for a 60 year design life. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-17: *The licensee shall generate the formal approved copy of the applicable Reactor Coolant Pump Design Specification for possible confirmatory assessment as normal regulatory business. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-18: *The licensee shall develop an adequate EMIT strategy for the AP1000 Reactor Coolant Pumps, with due consideration to the manufacturer's recommendations for preventative maintenance. Target Milestone – fuel on-site commissioning start as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-19: *The licensee shall generate evidence that the AP1000 proposed pump design can be installed and replaced with adequate consideration to UK legislation requirements and without having a negative impact on adjacent SSCs that are considered important to safety. This should also include justification for the use of temporary equipment (e.g. steel plates) during this process, as opposed to permanent features. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-20: *The licensee shall ensure that an appropriate safety classification is assigned to the RCP flywheel. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-21: *The licensee shall generate an adequate strategy for verifying the safety functional requirement of RCP flywheel coast-down performance during the operational lifetime of the NPP. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.13 Cranes

590 Lifting of nuclear packages or lifting operations over nuclear safety significant plant and equipment is an intrinsically hazardous, yet necessary activity within a Nuclear Power Plant, and I have continued my assessment in this important area. I consider the following Safety Assessment principles to be relevant to this area of assessment:

- Safety Assessment Principle ECS.3 (Ref. 4) states 'Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.'
- Safety Assessment principle EDR.1 (Ref. 4) states 'Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.'
- Safety Assessment Principle EDR.2 (Ref. 4) states 'Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.'

591 Specifically I have focussed my attention on the following four lifting systems, based on my consideration of their high safety importance:

- The main containment Polar Crane.
- The spent fuel pool area Cask Handling Crane.
- The main containment Re-fuelling Machine.
- The spent fuel pool area Fuel Handling Machine.

4.13.1 Assessment

4.13.1.1 Mechanical Design Features

592 I have questioned Westinghouse regarding the general Mechanical Engineering design and anticipated duty / usage of the four selected cranes (TQ-AP1000-188, Ref. 10) and they have provided the following information:

- The Polar Crane is designed for heavy lifts associated with the RPV, and the main and auxiliary hoists shall be Single Failure Proof and shall also comply with the guidelines of NUREG 0554 (Ref. 99) and ASME NOG-1 (Ref. 100) Section 5121 (Type 1 cranes). Both hoists shall be capable of withstanding the most severe overloads that can be imposed, including two blocking and load hang-up accidents, without loss of load control and without damage to the crane and hoisting components. For each hoist, a means shall also be provided for emergency lowering of the rated hoist load using the emergency brake.

- The Cask Handling Crane is designed for heavy lifts in the spent fuel pool area, specifically movement of the spent fuel cask. The main and auxiliary hoists shall be Single Failure Proof and shall also comply with the guidelines of NUREG 0554 and ASME NOG-1, Section 5121 (Type 1 cranes). Both hoists shall be capable of withstanding the most severe overloads that can be imposed, including two blocking and load hang-up accidents, without loss of load control and without damage to the crane and hoisting components. For each hoist, a means shall also be provided for emergency lowering of the rated hoist load using the emergency brake.
- The Refuelling Machine is designed for fuel handling operations associated with the RPV during outages. The main hoist is required to lift and transport 157 Fuel Assemblies (FA) from the reactor core to the fuel transfer system fuel carrier to support total core off load. The auxiliary hoist is used for handling operations associated with the control rod drive shafts. The refuelling machine hoist drive assembly is also equipped with a hand wheel to lower or raise the load in the event of hoist drive power failure.
- The Fuel Handling Machine is used for handling of new and spent fuel in the Spent Fuel Pool (SFP) area. This machine, which comprises a large frame structure which spans the pool has two attached hoists; a spent fuel hoist generally for handling of spent FAs within the SFP, and a new fuel hoist for handling of new FAs outside the pool. These hoists are also equipped with similar load recovery systems as for the Refueling machine hoists. However, Westinghouse has clarified that the new fuel hoist is Single Failure Proof, whereas the spent fuel hoist is non Single Failure Proof (TQ-AP1000-185 Ref.10). Westinghouse justified this on the basis that the new fuel hoist has the duty of lifting loads which are heavier than 1406 kg (this limit is associated with handling of FAs), and these are classified as heavy loads in US terminology, thus necessitating the use of a Single Failure Proof Hoist in the US nuclear crane selection system.

593 I have also questioned Westinghouse on the safety factors used within the four selected cranes, and although the initial response fell short of my expectations, I subsequently received an adequate quality response (TQ-AP1000-830, Ref. 10), which I have reviewed and consider to be acceptable from a Mechanical Engineering GDA perspective against SAPs ECS.3 and EDR.2.

594 I have also questioned Westinghouse regarding design for provision of loose article control, although I consider this to predominately be a matter for operational and specifically EMIT considerations. Westinghouse has confirmed (TQ-AP1000-405, Ref. 10) that this requirement is recognised through their design specifications, and I am satisfied from a GDA perspective against SAPs ECS.3 and EDR.2.

4.13.1.2 Control and Protection

595 Westinghouse provided information covering the control and protection philosophy applied to the light load handling system (TQ-AP1000-189, Ref. 10). They clarified that the light load system is Programme Logic Controlled (PLC) (Refueling Machine, Fuel Handling Machine), in contrast to the heavy load handling system (Polar Crane, Cask Handling Crane).

596 In response to questioning, Westinghouse confirmed that there is no separation between the control and protection functions for the light load handling system; both functions are effected through a single PLC. However, in the event of a PLC failure, the operator can recover the situation by 'manual' intervention. Westinghouse also stated that the

operator has the ability to hit an emergency stop. Westinghouse stated that this was a standard configuration for such a crane in the US.

597 I have now agreed that this topic will be taken forward by the C&I assessment discipline from a GDA perspective, in accordance with the planning protocol agreed for Step 4 assessment.

4.13.1.3 Rigging and Load Path Faults

598 I consider that the likelihood of mechanical failure due to inherent defects within the lifting systems to be very low, due to the rigorous quality assurance regimes to be applied during manufacture, and associated level of EMIT applied during the lifetime of the plant, including test lifts as appropriate. In this respect it should be noted that the Polar Crane is used extensively during the initial construction phase for installation of the Reactor Pressure Vessel Head, Reactor Vessel Internals, Reactor Coolant Pumps etc, and so any significant issues would be identified at this stage when there is no nuclear hazard. Operational Experience Feedback from the UK and also the IAEA Incident Reporting System (IRS) indicates that the great majority of nuclear lifting abnormal events are associated with operational errors. Initial discussions with Westinghouse identified that this area was not adequately recognised or justified to my expectations, and I continued to pursue this line of enquiry through the Step 4 process, specifically focussing on rigging and load path / route faults.

599 Westinghouse has now provided a more detailed response in respect of this line of enquiry, (TQ-AP1000-676, Ref. 10), which has addressed the questions in respect of rigging arrangements, and also load path / route determination. Westinghouse has also stated that a recent review of NUREG 1774 (Ref. 101) provides the following information:

- Based on actual crane operating experience data from commercial US NPPs the rate of load drops per demand for critical loads is 5.6×10^{-5} .
- Of the estimated 54000 critical load lifts at operating plants since issuance of NUREG-0612, three load drops were identified. These load drops were associated with human error / rigging deficiencies, and did not occur near any safety related areas of the plant.
- Of the estimated 54000 critical load lifts at operating plants since the issuance of NUREG-0612, six load slips were identified. None of the six critical load slips resulted in radiation releases or risk to the public.

600 Westinghouse are currently developing drawings identifying safe load paths for the handling of heavy loads that are of nuclear safety significance. Westinghouse has also made reference to their AP1000 In-Plant Design Criteria and Guidelines for the Control of Heavy Loads, (Ref. 82), which I have reviewed as part of my assessment. These drawings will be provided to the future licensee for incorporation into their heavy load handling programme. I consider it to be an Assessment Finding (**AF-AP1000-ME-22**) that this activity should be continued to a conclusion, and the load path determination should take into account ALARP principles. As an example Westinghouse has identified that a heavy lift involving the Cask Handling Crane is undertaken in a room above the Normal Residual Heat Removal Heat Exchangers, and Westinghouse presently rely of administrative controls only to ensure that the load path / route is clear of the area directly above these heat exchangers. I consider this to be a situation where physical barriers could be provided to prevent inadvertent handling of this heavy load over this sensitive area, and the practicability of provision of barriers should be reviewed on the basis of ALARP principles.

601 I consider it to be an Assessment Finding (**AF-AP1000-ME-23**) for a future licensee to ensure that all lifts of nuclear safety significance are identified, and safe load paths are specified through appropriate design and safety documentation, and procedures

602 I also consider it to be an Assessment Finding (**AF-AP1000-ME-24**) that the design of rigging equipment associated with lifts of nuclear safety significance is completed, and these designs are assessed to minimise the possibility of human error based on ALARP principles.

4.13.1.4 Spent Fuel Handling Hoist – RO-AP1000-058

603 I considered that the justification for the spent fuel handling hoist required further justification. This was on the basis that if a Single Failure Proof Hoist could be provided for the new fuel application, then justification was required as to why it could not also be provided for the spent fuel hoist on an ALARP basis, since a spent fuel assembly is intrinsically more hazardous than new fuel. I raised a Regulatory Observation, RO-AP1000-058 (Ref. 11) to pursue this matter, and this line of enquiry is described in the following paragraphs.

604 Regulatory Observation RO-AP1000-058 states:

- Assessment to date of the Fuel Handling Machine (FHM), part of the light load handling system within the AP1000 design, has identified insufficient justification for the design of the spent fuel handling hoist, as being non-Single Failure Proof. Westinghouse is required to provide an adequate justification to satisfy this shortfall.

The RO also placed the following action on Westinghouse:

- Westinghouse to provide an adequate justification as to why they consider it to be ALARP, to not provide a Single Failure Proof spent fuel handling hoist for the Fuel Handling Machine (FHM).

605 This subject area was discussed across a number of technical meetings with Westinghouse in Pittsburgh, and they provided a first response to this RO in April 2010, which was subsequently revised to account for my comments and re-issued in August 2010 (Ref. 11). In this RO response Westinghouse make the following points:

- The likelihood of a load being dropped is minimised by the following crane design features:
 - i) Overload features to stop the hoist in the event of load 10% greater than anticipated load being detected.
 - ii) Redundant components or conservative design margins.
 - iii) Dual brakes, both designed to hold 150% of the rated load.
 - iv) Dual load weighing system.
 - v) Dual absolute position encoders for each axis of motion.
 - vi) Redundant hoist up limit switch.
 - vii) Hoist wire rope rating is sufficient to support five times the design load.
 - viii) Hoist capacity is circa 70% higher than the loads associated with the handling of spent fuel.

606 Westinghouse has also described the consequences of a dropped Fuel Assembly (FA), and specifically stated that because of the length of the spent fuel handling tool it is not

physically possible to drop the spent FA from a height greater than 300 mm above the fuel storage rack; i.e. the drop height is constrained by design. They have also referred to fuel drop tests performed by themselves from heights of 3m and 6m in water. They have also discussed drop tests undertaken in the UK. Based on this evidence Westinghouse has stated that the potential for FA cladding damage is very small from the maximum credible drop height of a spent FA.

- 607 They have also referred to OEF from the Institute of Nuclear Power Operators (INPO) which listed circa 300 events associated with fuel assembly damage. Westinghouse has identified seven events associated with dropped FAs. None of these events resulted in fuel cladding damage or any release of radioactivity, and only one was associated with the failure of the hoist.
- 608 Westinghouse has also stated through discussion that all spent fuel handling hoists in the US are non Single Failure Proof.
- 609 Westinghouse has discussed the potential impact of moving to a Single Failure Proof hoist, noting that this would require a more complex cross reeved design, to ensure that loads on the lower crane block remain balanced in the unlikely event of a rope rupture. This would require a significantly larger, heavier, and more costly hoist design, with lower hoisting speeds of approximately half of those for the present design. In respect of lower hoisting speeds, Westinghouse has stated that this will increase outage time, and hence lead to increased operator doses. Westinghouse quote an increase of circa 8 hours for each outage, which I recognise has a detrimental commercial effect, and is a valid parameter in the ALARP argument. I consider the increase in associated operator dose to be small but significant.
- 610 Westinghouse has also confirmed through discussion and correspondence (TQ-AP1000-1215, Ref. 10) that the reeving system for the spent fuel hoist is a dual reeved design (to ensure that the load moves in a purely vertical direction on lifting / lowering), and the design uses two ropes attached via a balance plate at the dead end. They have stated that the arrangement will still support the load by one rope in the event of failure of the other, although single rope failure will result in slight slippage of the load. This statement is supported by the rope rating safety factor of five, such that in the event of failure of a single rope, a minimum safety factor of 2.5 is achieved, before accounting for any dynamic effects.
- 611 I have also reviewed the equivalent lifting hoist for the Sizewell B NPP and have concluded it is of a similar design to that proposed by Westinghouse, and specifically it is not Single Failure Proof either (to the definition of the recognised standards).
- 612 After further consideration, and based on the arguments and evidence put forward by Westinghouse, including comparisons to existing design and review of OEF, I am now content in respect of this topic, and accept that the spent fuel hoist design is acceptable from a GDA perspective against SAPs ECS.3 and EDR.2.

4.13.2 Findings

AF-AP1000-ME-22: *The licensee shall ensure that the AP1000 load path determination activity is completed, and this load path determination should take into account ALARP principles. In particular Westinghouse has identified that a heavy lift involving the Cask Handling Crane is undertaken in a room above the Normal Residual Heat Removal Heat Exchangers, and the design presently relies on administrative control only to ensure that the load path / route is clear of the area*

directly above these heat exchangers. I consider this to be an example of where physical barriers could be provided to prevent inadvertent handling of this heavy load over this sensitive area, and the practicability of provision of barriers should be reviewed on the basis of ALARP principles. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

AF-AP1000-ME-23: *The licensee shall ensure that all lifts of nuclear safety significance are identified, and safe load paths are specified through appropriate design and safety documentation, and procedures. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-24: *The licensee shall ensure that the design of rigging equipment associated with lifts of nuclear safety significance has been completed, and these designs have been assessed to minimise the possibility of human error based on ALARP principles. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.14 Nuclear Ventilation

613 Nuclear ventilation systems play an important role in an NPP in controlling the spread of radioactive contamination in normal and accident conditions, and directing any discharges to suitably filtered routes.

614 In particular I have assessed the following technical aspects of the nuclear ventilation system:

- Provision of Passive HEPA Filtration.
- Design and Testing of HEPA Filtration.
- Emergency Habitability Systems.
- Provision to accommodate the UK Maritime Climate.
- Nuclear Ventilation Design Temperatures.
- Nuclear Ventilation Stack Height

615 I consider the following Safety Assessment Principles to be relevant to the subject of nuclear ventilation, and I have used them to guide my assessment accordingly:

- Safety Assessment Principle ECV.3 (Ref. 4) states 'The primary means of confining radioactive substance should be by the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components'.
- Safety Assessment Principle AM.1 (Ref. 4) states 'A nuclear facility should be so designed and operated to ensure that it meets the needs of accident management and emergency preparedness.'

- Safety Assessment Principle EAD.2 (Ref. 4) states 'Adequate margins should exist throughout the life of a facility to allow for the effects of materials aging and degradation processes on structures, systems and components that are important to safety.'
- Safety Assessment Principle EHA.11 (Ref. 4) states 'Nuclear facilities should withstand extreme weather conditions that meet the design basis event criteria'.
- Safety Assessment Principles EKP.3 (Ref. 4) states 'A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several layers of protection'.

4.14.1 Assessment

4.14.1.1 Provision of Passive HEPA Filtration

616 As a large part of my Step 4 assessment activity within the field of nuclear ventilation, I have pursued the provision of passive HEPA filtration within the AP1000 nuclear ventilation system designs. My Step 3 review indicated there were significant shortfalls in this area, and I raised an associated Regulatory Observation in September 2009 (Ref. 11). This RO which was developed in conjunction with the Environment Agency is stated as follows:

- Assessment to date of the nuclear ventilation systems for the AP1000 design has identified insufficient justification for the proposed HEPA filtration arrangements for each and all ventilations systems which have the potential for significant airborne contamination under either normal or fault conditions, to meet UK Regulatory expectations. Westinghouse is required to provide an adequate justification to satisfy this shortfall.

This Regulatory Observation also addressed my concern over the lack of an adequate safety justification, including safety function categorisation and equipment classification for the equipment comprising the nuclear ventilation systems. I raised the following actions on Westinghouse as part of this RO:

- Westinghouse should provide a justification as to why they consider it to be ALARP, and in line with good nuclear engineering practice, to not provide passive HEPA filtration for each and all ventilations systems which have the potential for significant airborne contamination under either normal or fault conditions.
- The Westinghouse should provide an appropriate and adequate nuclear safety evaluation, for all ventilation systems which have the potential for significant airborne contamination under either normal or fault conditions.
- The Westinghouse should identify and classify all structures, systems and components that have to deliver safety functions within the nuclear ventilation systems.

617 This subject was discussed at length throughout the Step 4 process. During technical meetings I stated that there was a clear expectation that there should be passive HEPA filtration based on UK relevant good practice, as described in the RO and associated explanation. Westinghouse described the various ventilation arrangements for the main room spaces, and stated that the systems were typical of those utilised in the US. However, in response to questioning, Westinghouse confirmed that they had not undertaken a comparison to UK or European practice in respect of nuclear ventilation,

and I suggested they should consider this as part of their work in developing the RO response.

618 I also commented on the societal impact of any radioactivity releases, which was an important factor in my assessment of this topic area.

619 I advised that in developing, or testing their ALARP justification, Westinghouse should consider the option of providing additional passive filtration, and then consider whether or not the associated 'money, time or trouble' is grossly disproportionate; although I stated that I was not looking for a cost benefit analysis, but simply qualitative arguments.

620 Westinghouse finally produced what I now consider to be a satisfactory response to this RO in August 2010, and their design change proposals are summarised as follows:

- VHS modifications (health physics and hot machine shop) – VHS fans will now stop on a high radiation signal from duct mounted and / or area radiation monitoring, and exhaust through the VFS: the airflow from the health physics and hot machine shop will therefore be reduced, but the exhaust will thus be HEPA filtered. Previously no filtration was applied to the room exhaust air. The VHS high efficiency filter in the machine tools local exhaust ventilation arrangements will be replaced with a more effective HEPA filter.
- VRS modifications (radwaste building) – HEPA filtration will be added to the VRS exhaust from the radwaste building. Previously no filtration was applied to the exhaust air.
- VAS modifications (radiologically controlled area) – Auxiliary building area radiation monitors will be added to the controls that isolate VAS and actuate VFS filtration. The VFS provides a discharge route which is both iodine and HEPA filtered, but the response time of this changeover is now improved due to the addition of area radiation monitors to the controls that isolate VAS.
- VAS Fuel Handling Area (spent fuel pool) – Full time HEPA filtration is now being incorporated into the design. Previously passive HEPA filtration was not applied within the normal discharge route, and although the VAS would switch over to the VFS on a high radiation signal, this relied on an active system, and there would be a small time lag until this occurred.

Although there is still some reliance on active systems to effect nuclear ventilation filtration, I am now satisfied that adequate passive filtration is incorporated within the design against SAP ECV.3. Furthermore, active systems are required in some systems to effect iodine filtration, since these rely on a chemical cleaning process, and I consider it is not reasonably practicable to use this on a continuous basis.

621 I am now also satisfied that Westinghouse has recognised the safety importance of the nuclear ventilation systems, as an outcome of the overall realignment of their safety case to meet UK expectations. I also recognise that they have now classified the associated SSCs in their response to the topic of safety function categorisation and equipment classification (Ref. 35).

622 I have reviewed the DCPs associated with these design changes (TQ-AP1000-1201, Ref. 10), and I am now satisfied in this respect. However, I consider it to be an Assessment Finding (**AF-AP1000-ME-25**) that these changes are progressed and all necessary AP1000 design and safety documentation is updated accordingly.

623 In December 2010 Westinghouse briefly explained the design for the HEPA filters associated with the spent fuel pool 'blow out panels'. These features are designed to act

as safety systems to alleviate the infrequent fault of pressurisation of the spent fuel pool area, caused by loss of cooling to the pool and hence boiling of the pool water. They stated that these 'panels' are actually temperature operated dampers, which are designed to operate at circa 75 degrees Celcius, which then lead to HEPA filters and external discharge. Westinghouse stated that such HEPA filters are perfectly adequate to deal with saturated steam at atmospheric pressure, although arrangements for collecting condensate would need to be incorporated into the design. I have not specifically assessed this design since it has derived from recent work (with assessment led by the Fault Studies discipline), and as such I consider it to be Mechanical Engineering Assessment Finding (**AF-AP1000-ME-26**).

4.14.1.2 Design and Testing of HEPA Filtration

- 624 I decided to assess the detailed design and testing of HEPA filters used within the AP1000 design, since these provide the important safety function of containment of radioactive substances, specifically in the event of postulated accidents within the NPP.
- 625 Westinghouse provided information in respect of testing of HEPA filtration, referring to the standard filter efficiency of 99.97% for the Most Penetrating Particle Size (MPPS) of 0.3 µm. HEPA filters are procured in accordance with ASME N509, Nuclear Power Plant Air-Cleaning Units and Components.
- 626 The ASME code requirements stipulate that each filter design requires factory qualification tests (type tests) for:
- Airflow resistance.
 - Test aerosol penetration.
 - Resistance to rough handling.
 - Resistance to pressure.
 - Resistance to heated air.
 - Spot flame resistance.
- 627 Furthermore, the code requires the re-qualification of filter designs every five years. In addition, each individual filter is factory tested for test aerosol penetration, and airflow resistance.
- 628 Westinghouse stated that the actual filter efficiency used in calculations is 99%, which I consider is in line with standard nuclear safety practice to use a lower value for safety calculations. It should be noted that HEPA filters typically have efficiencies of 99.97%.
- 629 In response to my questions, Westinghouse stated that they were not aware of any recent adverse OEF with regard to HEPA filters. Westinghouse commented that although they recognised that circular filters had some potential advantages in respect of sealing due to their shape and hence seating within the housing, and that difficulties were sometimes experienced at the corners for rectangular filters, these rectangular filter types were heavily used in the US and were the basis of the AP1000 design. I am satisfied with this response from a GDA perspective.
- 630 The Differential Pressure (DP) is measured across all filter banks, which is automatically monitored and alarmed, albeit not for the emergency habitability system. I accept that since the emergency habitability system is not routinely used, and therefore not subject to filter blinding, it is not reasonable to provide this facility for these filters.
-

- 631 Westinghouse also described the in service testing requirements for HEPA filtration, noting the code requires testing after each HEPA filter replacement, and at least once each operating cycle. I consider that the filter change philosophy should obviate the need for system re-balancing as the filters start to 'clog' during their operational usage. I consider it to be an Assessment Finding (**AF-AP1000-ME-27**), that a future licensee establishes an appropriate filter change doctrine for all safety important filters within the nuclear ventilation systems
- 632 In summary, I consider that Westinghouse's description of their technology in respect of HEPA filter performance and testing is in line with my expectations against SAP ECV.3, and I am satisfied in this area from a GDA perspective.

4.14.1.3 Emergency Habitability Systems

- 633 The Emergency Habitability Systems for the Main Control Room have important safety functions in the event of a release of radioactive contamination from the NPP, to ensure that adequate protection is provided to allow the plant operators to undertake any necessary actions. I have therefore targeted my assessment in this area. I had made initial enquiries in this respect during Step 3 (TQ-AP1000-193, Ref. 10).
- 634 The system basically is passive, using compressed air and air eductors (amplifiers), to pressurise the control room through HEPA and iodine filtration. The eductors are fed by compressed air, and draw in air from outside the room by a partial vacuum effect, achieving an airflow magnification of approximately ten compared to the compressed air flow itself. Westinghouse has stated that there is some development work associated with the air eductors, but the whole system will be tested as part of the commissioning tests.
- 635 The system is designed to operate to full design requirements for 72 hours following a Design Basis Accident / loss of AC power, with a degraded requirement following this timescale.
- 636 The filtration system comprises a HEPA filter, then a charcoal filter (iodine trap), and a final post filter to capture charcoal particles etc. The air is then fed into the main control room. Both the HEPA and charcoal filters are designed to be replaced, as panel filters.
- 637 The filters have no redundancy built into their design, noting that they are passive features. The design philosophy is to maintain and replace the filters during cold shutdown periods (noting that the time to change the filters would be less than 1 hour). Westinghouse commented that for twin station areas, then there would have to be time restrictions associated with filter changing.
- 638 I decided to extend this line of enquiry to assess the postulated accident scenarios associated with the use of the MCR Emergency Habitability System, and extended the remit to cover supplementary control rooms, and the Control Support Area used for command and control in the event of an emergency (TQ-AP1000-543, Ref. 10).
- 639 In particular, the Control Support Area is ventilated by the same system that serves the MCR. However, the Remote Shut-down Room (supplementary control room) ventilation system does not have HEPA or iodine filters, since the primary use for this facility is in the event of a fire in the MCR.
- 640 I have discussed these fault scenarios and associated frequencies with my PSA assessment colleagues, and discussed the levels of protection it is reasonable to expect for these fault scenarios. In conclusion, I am now satisfied with the explanations provided by Westinghouse and the design principles for the MCR Emergency Habitability Systems,

and associated provision for the supplementary control room, and the Control Support Area, against SAP AM.1.

4.14.1.4 UK Maritime Climate

641 I questioned Westinghouse regarding the 'hardening' of the nuclear ventilation design external features to accommodate the harsh UK maritime climate, (TQ-AP1000-197, Ref. 10), specifically in respect of corrosion. Westinghouse initially responded that they were considering changes to the nuclear ventilation external features to account for the UK maritime weather/climate. I have pursued these changes through the GDA Step 4 process, which are summarised as follows:

- Use of marine grade aluminium or other suitable material for intake ductwork and louvers up to the air-handling unit's filters for most ventilation systems.
- Add aspirating model smoke detectors in the intake ducts that will not actuate on foggy days.
- Specify that the exhaust fan and intake louvers be covered with the manufacturer's marine / coastal coating for the Turbine Building Ventilation System (VTS) and the use of marine grade aluminium or other suitable material for the air-handlers intake ductwork and louvers up to the filter.
- Add filters to protect the air compressors in the Containment Leak Rate Test System.
- Specify that the equipment within the turbine building be covered with the manufacturer's marine / coastal coating for the Central Chilled Water System and Hot Water System.
- Specify that fans and other ventilation equipment located on the roof have the manufacturer's marine / coastal coating.

642 Through discussion, Westinghouse indicated that generally these changes are only proposed for UK maritime sites, and therefore are not applicable for any inland AP1000 NPPs to be constructed in the UK. I consider that all the proposed sites presently identified in the UK are near the shoreline, and I consider it unlikely that any NPPs will be constructed significantly inland. I consider that Westinghouse should clearly identify within their design and safety documentation that these features are a design requirement for maritime sites, to avoid any misunderstanding.

643 I have now reviewed the DCP associated with these design changes (TQ-AP1000-1201, Ref. 10; APP-GW-GEE-767, Ref. 84), and Westinghouse has confirmed that the following changes have now been approved via the DCP process, and are therefore incorporated into the UK AP1000 standard design:

- Add aspirating model smoke detectors in the intake ducts that will not actuate on foggy days.
- Add filters to protect the air compressors in the Containment Leak Rate Test System.

However, I consider it to be an Assessment Finding (**AF-AP1000-ME-28**) that these changes are progressed and all necessary AP1000 design and safety documentation is updated accordingly.

644 Westinghouse has stated that the other changes considered necessary to harden the ventilation systems will be described as expected changes for coastal sites in the update of the PCSR due at the end of the GDA process. Although I would prefer that these were

identified within the standard AP1000 design for the UK, I don't consider it proportionate to pursue this further within GDA. However, I consider it to be an Assessment Finding (**AF-AP1000-ME-29**) that these changes are implemented for the AP1000 design for UK coastal site applications.

4.14.1.5 Nuclear Ventilation Design Temperatures

645 I have also questioned Westinghouse regarding the design temperatures associated with the nuclear ventilation system, to ensure that they are appropriate and adequate for the UK, for the AP1000 60 year design life.

646 Westinghouse provided information on the AP1000 design safety temperatures (TQ-AP1000-196, Ref. 10), as max. 46.1 degree C dry bulb, min. minus 40 degree C. Westinghouse has compared these values to the 100 year maximum and minimum return values for two of the proposed UK sites, Wylfa and Oldbury, and determined that these sit within the design values; (although further work will be undertaken in this area, and the maximum humidity (wet bulb temperature) at Oldbury will be subject to further investigation/verification) .

647 In response to my questions, Westinghouse stated that if temperatures outside the design safety values are experienced, then the plant will have to shut down. However, they also clarified that in the event of temperatures beyond design being experienced, there would be a gradual degradation in performance of the nuclear ventilation system, without cliff edge type effects. I agree that this is a reasonable assertion.

648 I have also questioned Westinghouse in respect of the temperatures in the spent fuel pool area (TQ-AP1000-423, Ref. 10), to gain an understanding of the capacity of the nuclear ventilation systems to provide a reasonable working environment for operators. The specific ventilation system dedicated to this area has been designed to maintain the pond area temperature at between 10 degrees C and 35 degrees C (dry bulb) in worst case conditions. However, normal room temperatures will generally be circa 20~25 degrees C. Recognising that this is not a routinely occupied area, and that the extreme temperatures are based on worst case conditions (specifically outside air temperatures), I consider this approach to be reasonable.

649 I also consider that the AP1000 design temperatures for the nuclear ventilation system should be reviewed on a site specific basis, once the sites for the proposed UK AP1000 NPPs have been determined, which I consider to be an Assessment Finding (**AF-AP1000-ME-30**).

650 I am satisfied with the explanations provided by Westinghouse in terms of general design parameters for the nuclear ventilation system against SAP EHA.11, and recognise that the AP1000 has been designed for worldwide application in this respect.

4.14.1.6 Nuclear Ventilation Stack Design

651 I have also reviewed the nuclear ventilation stack design, specifically the height of this ventilation stack, and comparison to relevant good practice in the UK. This stack is the discharge point for the nuclear ventilation systems within the AP1000, and its height is an important parameter in ensuring adequate dispersal of radioactive contamination under potential fault conditions; (albeit it should be understood that such discharges are subject to iodine and particulate filtering within the ventilation systems themselves).

- 652 Although the final design confirmation of the nuclear ventilation stack is a Phase 2 matter, I considered it appropriate to undertake a limited assessment in this area, in respect of the generic features of the stack design (specifically its height).
- 653 During Step 4 technical meetings I discussed the response to the technical query raised in relation to the AP1000 nuclear ventilation stack height, (TQ-AP1000-555, Ref. 10). This response stated that the stack finishes 15 to 20 metres below the top of the containment / shield building structure. I commented that I was aware that the Chinese Regulator had required Westinghouse to raise the stack to at least 5m higher than this adjacent building, which Westinghouse confirmed. I also referred Westinghouse to UK document 'An Aid to the Design of Ventilation of Radioactive Areas', (Ref. 71), which states that, 'in general, for the full stack height to be effective, it must be significantly higher than the tallest building in the immediate vicinity'.
- 654 Westinghouse tabled the stack design height modification for the Chinese project for information. I stated that the final stack height would depend on local buildings and topography, but from a GDA perspective it was difficult to accept the apparent AP1000 standard proposal. Westinghouse agreed to review this matter, and I decided to raise a further technical query (TQ-AP1000-730) to progress this topic.
- 655 Westinghouse has now responded to this technical query, and has agreed that it is ALARP to raise the ventilation stack height to a level circa 5m above the main containment building structure. Although I consider that the final confirmation of the nuclear ventilation stack height is a site specific matter, I am now satisfied that the GDA AP1000 design is adequate as a basis for this site specific confirmation against SAP EKP.3.
- 656 I have reviewed the DCP associated with this design change (TQ-AP1000-1201, Ref. 10), and am now satisfied in this respect. However, I consider it to be an Assessment Finding (**AF-AP1000-ME-31**) that this change is progressed and all necessary AP1000 design and safety documentation is updated accordingly.

4.14.2 Findings

AF-AP1000-ME-25: *The licensee shall ensure that the design changes associated with the provision of passive HEPA filtration for the nuclear ventilation systems in response to RO-AP1000-043 have been completed and that all necessary AP1000 design and safety documentation has been updated accordingly. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-26: *The licensee shall ensure that an adequate design substantiation has been generated for the ventilation design changes, specifically 'blow out panels', made in response to the Regulatory Observation regarding the Spent Fuel Pool DBA requirement (RO-AP1000-054, Ref. 11). Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-27: *The licensee shall establish an appropriate filter change doctrine for all safety important filters within the nuclear ventilation systems. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and*

Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

AF-AP1000-ME-28: *The licensee shall ensure that design changes (APP-GW-GEE-767) associated with the 'hardening' of the nuclear ventilation external features to accommodate the UK maritime climate / weather have been completed and that all necessary AP1000 design and safety documentation has been updated accordingly. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-29: *Westinghouse has stated that further changes considered necessary to harden the ventilation systems will be described as expected changes for coastal sites in the update of the PCSR due at the end of the GDA process. The licensee shall ensure that these changes are implemented for the AP1000 design for UK coastal site applications. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-30: *The licensee shall verify the site specific design air temperatures and humidity values against those used as the basis for the AP1000 design, to ensure that the nuclear ventilation systems can adequately perform their safety functions. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-31: *The licensee shall ensure that the design change associated with the increase in nuclear ventilation stack height has been completed and that all necessary AP1000 design and safety documentation has been updated accordingly. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.15 Gloveboxes and Cabinets

657 I have undertaken a limited review of gloveboxes and cabinets as part of my assessment, which have the safety function of containment of radioactive substances, (TQ-AP1000-198, Ref. 10).

4.15.1 Assessment

658 Westinghouse has provided a response to this technical query, and has also clarified in response to RO-AP1000-043 (Ref. 11) that the glovebox used within the health physics and hot machine shop will be provided with HEPA filtration, in line with my expectations.

659 It should be noted that any fume cupboards within the AP1000 design are not appropriate for containment of radioactive materials, and I consider it to be an Assessment Finding

(**AF-AP1000-ME-32**) that a future licensee restricts their use to appropriate chemical hazards only.

660 There is a limited requirement for this type of equipment within the AP1000, and it represents a mature technology. I have also covered this area as part of my assessment of the AP1000 nuclear ventilation systems, described elsewhere in this report. I have not identified any concerns regarding gloveboxes and cabinets as part of my assessment.

4.15.2 Findings

AF-AP1000-ME-32: *The licensee shall ensure that any fume cupboards within the AP1000 are not used for the containment of radioactive substances. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components -inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.16 Heat Transfer and Heat Exchangers

661 I have assessed the Mechanical Engineering features of the heat transfer systems and equipment used within the AP1000 design, which provide the important safety function of heat transfer and removal for both nuclear and decay heat from the reactor core, under both normal and fault conditions.

662 I consider the following Safety Assessment Principles to be relevant to this assessment area:

- Safety Assessment Principle EHT.1 (Ref. 4) states 'Heat transport systems should be designed so that heat can be removed or added as required.'
- Safety Assessment Principle EHT.3 (Ref. 4) states 'A suitable and sufficient heat sink should be provided.'
- Safety Assessment principle EDR.1 (Ref. 4) states 'Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.'

4.16.1 Assessment

4.16.1.1 Normal Residual Heat Removal System

663 I have assessed the Normal Residual Heat Removal System (RNS), due to its important safety functions of heat transfer and removal during both normal and fault conditions. The system is designed to remove decay heat from the core once the reactor has been shut down following insertion of the control rods.

664 My assessment has targeted the RNS system following discussion with the Fault Studies assessor, the issue of RO-AP1000-047, and the system's considered safety significance.

665 Westinghouse has provided information describing the RNS and explained that the system has several safety functions, TQ-AP1000-1269 (Ref. 10). These are described as follows:

- Safety Function Category A and Equipment Classification 1:

-
- i) Maintaining RCS pressure boundary during normal operations with valves V001 A/B, V002A/B, V015 A/B, and V017A/B providing the principle means of isolation (containment safety function).
 - ii) Providing isolation during conditions when the RNS is open to the RCS (with the exception of the shell side of the RNS heat exchanger): i.e. suction line valves V002 A/B, V021 A/B, V022A/B, V023A/B and V061 A/B, and discharge line valves V011A/B and V013 A/B provide the principle means of isolation (containment safety function).
 - iii) Low Temperature Overpressure Protection (LTOP) for the RCS during refuelling and during shutdown operations, which is also covered by an associated Technical Specification.
- Safety Function Category A and Equipment Classification 2:
 - i) During a shutdown or a post accident heat removal scenario, the RNS provides a closed loop heat removal from the RCS.
 - ii) During a shutdown or Mid Loop operation, the RNS provides shutdown decay heat removal both during refuelling operations and during a reduced inventory scenario.
 - iii) In a low pressure RCS scenario, the RNS has a provision to inject at low pressure from either the Cask Loading Pit or the IRWST.
 - iv) During long term post accident containment recirculation, the RNS provides provision to cool water, which is drawn from containment and re-circulated through the pressure vessel.
 - v) Provision to provide extra capacity to cool the spent fuel pond during spent fuel system train maintenance and during a full core off load.
 - vi) During shutdown the RNS is able to provide purification capacity of 100 gallons per minute flow through the CVS.
 - vii) Ability to cool the IRSWT during plant operation and / or the Passive Residual Heat Removal Heat Exchanger. Both trains are required to maintain the IRSWT below boiling. The IRSWT cooling is required if the Main Feedwater system malfunctions.
- 666 The system design incorporates redundancy, diversity and segregation. Redundant connections are provided for the following aspects:
- IRWST containment sump.
 - Spent Fuel Pool.
 - CVS for shutdown and purification.
 - LTOP protection, (valves V021 A/B).
- 667 In response to questions, Westinghouse identified that the RNS suction line valves are located in separate rooms to provide a fire and flood barrier. Each valve has 4 different DC power supplies. The system design arrangement incorporates 2 separate suction and discharge containment penetrations. The RNS heat exchangers and control valves are located in separate rooms, again to provide fire protection, and the two train pumps and associated valves are also located in two individual rooms.
- 668 The RNS system has some automated aspects but it is not a fully automated system. Automated aspects include:
-

-
- The containment isolation valves.
 - RCS cooldown is automated via valve (V006A/B and TE13A/B) and (V008A/B, FT001A/B).
 - Pump protection is provided by valve V057A/B, which opens automatically on low flow.
 - CVS demineraliser protection is provided by V0299, which closes automatically on a high temp signal.
 - Pumps are connected to the diesel generators and start up automatically in a loss of offsite power, provided the RNS is aligned for shutdown cooling.
- 669 Discussion on surveillance and testing requirements confirmed that the system has a number of Technical Specifications associated with it; for example:
- TS 3.4.14 Low Pressure Overpressure Protection requires EMIT on system alignments and pressure relief valve testing.
 - TS 3.4.15 RCS valve isolation, integrity and leak rate verification.
 - TS 3.6.3 Valve containment isolation verification.
- 670 In-service testing requirements for containment isolation and safety relief valves are set in accordance with ASME code requirements, and are periodically tested by verifying their:
- Remote position indication.
 - Leak rate.
 - Ability to operate and function to their design intent.
- 671 The system design incorporates a two valve arrangement to provide system isolation. This is achieved either via check valves or motor operated valves, which I considered to be in line with my expectations.
- 672 The system is of a two train design, which can allow one train to support core cooling requirements, while the other train is able to support the spent fuel pool cooling requirements (for example).
- 673 The system generally has multiple roles and is sized for each train to typically operate individually, rather than both trains in parallel. However, the system has provision to maintain the fluid level within the CMTs. In this scenario both trains are required to be used, so redundancy is not provided in this aspect by the RNS trains.
- 674 Westinghouse stated that EDCD Chapter 16.3 captures these requirements from a GDA perspective and information will also be provided in response to Regulatory Observation RO-AP1000-094 (Ref. 11), which aims to understand how the Plant Operating Rules, Operating Technical Specifications and Maintenance Schedules can be derived from the design basis limits and conditions, and the associated PCSR claims.
- 675 In response to questions on considerations to operational experience Westinghouse stated that the AP1000 has incorporated OEF from several sources, which include:
- Considerations from utility feedback.
 - Utility participation in the design process and design reviews of both the AP600 and AP1000 NPP designs.
-

- Nustart Energy Development participation throughout the Westinghouse design process.
- Consideration to various regulatory assessment requirements.
- Consideration to Japanese operating experience feedback via the Simplified PWR design development with Mitsubishi Heavy Industries.
- WCAP-14115 Rev 0 (Ref. 39) Review of nuclear plant operating experience and the application to the AP600 design.
- APP-GW-G1R-007 Rev A (Ref.40) Operating experience to apply to Advanced Light Water Reactor designs.
- WCAP-15800 Rev 3 (Ref.41) Operational assessment for AP1000.
- WCAP-14645 Rev 3 Human factors, engineering operating experience review report for the AP1000 NPP.

676 In summary, I am satisfied with the explanations provided by Westinghouse on the RNS system from a Mechanical Engineering perspective against SAPs EHT.1 and EDR.1.

4.16.1.2 Component Cooling Water System

677 I decided to assess the Component Cooling Water System, due to its important safety functions of heat transfer and removal during both normal and fault conditions. As part of this assessment, I have also reviewed the provision of ultimate heat sink for nuclear island cooling requirements.

678 The key safety functions of the Component Cooling Water System (CCS) are as follows:

- Removes heat from plant equipment.
- Normal heat removal path for reactor core and spent fuel decay heat.
- Supports long term recovery of plant from accidents following activation of Passive Core Cooling Systems.
- Provides other functions, such as IRWST cooling after Passive Residual Heat Removal Heat Exchanger actuation, and Reactor Coolant System heat removal during reduced coolant volume operation.

679 Westinghouse stated that failure of the CCS is considered in the PRA since its failure leads to an initiating event, and it is also used as a support system for other systems credited in the PRA.

680 The CCS system comprises two parallel trains, with redundancy in respect of normal power heat removal capacity, physical separation of key redundant components by train, and train cross connections for maintenance and repair flexibility. The system also has the capacity to isolate the normal equipment cooling path from that required for decay heat removal (covering the residual heat removal system, and spent fuel pool cooling heat exchangers).

681 The cooling capacity of the CCS is summarised as follows:

- Plant cooldown is possible with only one train of CCS available, but the duration is extended.

- Operation of both cooling trains can maintain the refuelling water temperature at or below 48.9°C (based on a 27°C external wet bulb temperature, which limits the Service Water System cooling tower performance).
- Operation of both trains can maintain spent fuel pool water temperature at or below 48.9°C for full core off-load.
- Operation of one train can maintain spent fuel pool water temperature at or below 48.9°C for a normal refuelling.

682 I subsequently raised a technical query on Westinghouse, to gain a better appreciation of the overall cooling train from the Spent Fuel Pool and RNS system, through to the CCS, and then through to the SWS, and to gain an understanding of the fault tolerance of these systems, (TQ-AP1000-675, Ref. 10). In response to this technical query, Westinghouse described the following scenarios to describe the fault tolerance of the system:

- At power – single failure in Spent Fuel Pool Cooling System (SFS).
- Shutdown – single failure in SFS.
- Shutdown – single failure in RNS.
- Shutdown – single failure in CCS and SWS.
- Refuelling – no failure.
- Refuelling – single failure in SFS.
- Refuelling - single failure in CCS and SWS.
- Start-up – no failure.
- Start-up – single failure in SFS.

In terms of the spent fuel pool temperature, the worst case occurs during refuelling with a single failure in CCS and SWS. In this case the SFP temperature rises to 61.1 degrees Celsius. This assumes two SFS trains aligned for spent fuel pool cooling, but only one CCS / SWS train. The heat load in the SFP assumes 15 years of old fuel, plus 157 FAs recently offloaded from the reactor. Westinghouse has also stated that this is a very conservative case due to operational constraints. In respect of the above failure combinations, I note that the predicted temperatures are based on a site wet bulb temperature of 26.7 degrees Celsius, and 30.1 degrees Celsius for the first case; (noting that these wet bulb temperatures are equivalent to the stated air temperatures at 100% humidity, or higher air temperatures at lower levels of humidity).

683 I am aware that the GDA fault studies discipline have raised concerns regarding the design basis safety justification for the SFP and for shutdown conditions, (RO-AP1000-054, Ref. 11), and are pursuing this area to ensure that the predicted frequency of SFP boiling is acceptably low, in the event of faults within the identified cooling trains. Notwithstanding this, I am satisfied with the explanations provided by Westinghouse in terms of heat transfer capability from a Mechanical Engineering perspective, although I consider it to be an Assessment Finding (**AF-AP1000-ME-33**) that the RNS / SFP heat transfer calculations are reviewed against the site specific predicted temperatures / conditions, as a Phase 2 activity.

684 Westinghouse also described some ALARP considerations associated with the design of the CCS from a radiation perspective, stating that it is a closed system, not connected to the RCS or other sources of activity, and that a sensitive liquid radiation monitor is placed on the CCS pump suction header.

685 In response to questions, Westinghouse confirmed that the design life of the CCS is 60 years, with the principal material of construction being carbon steel, based on an appropriate chemical dosing regime. In response to further questions, (TQ-AP1000-679, Ref. 10), Westinghouse has stated that this choice has been based on considerations of:

- Cost.
- Mechanical strength.
- Corrosion considerations, including use of a suitable chemical treatment regime, and suitable design allowances on material thickness.

Westinghouse has stated that carbon steel is the material selected for the CCS for the majority of PWRs in the Westinghouse fleet.

686 I am satisfied with the response received in respect of the CCS material of construction, but I consider it to be an Assessment Finding (**AF-AP1000-ME-34**) that a future licensee assesses the practicability of inspecting and / or replacing detrimentally affected sections of the CCS in respect of corrosion, and implement any necessary ALARP improvements which are identified.

687 I have reviewed the latest version of the AP1000 safety function categorisation and equipment classification document (Ref. 35) in respect of the CCS and am satisfied that this system has been adequately captured from a GDA perspective. Westinghouse has also described the Examination, Maintenance, Inspection and Testing arrangements applicable to the CCS in general terms, which I considered to be reasonable from a GDA perspective.

688 Westinghouse stated that the CCS design has been undertaken with reference to the Utility Requirements Document for the AP1000, plus relevant operational experience from US and European utilities and the US NRC, and these aspects are included in the intermediate and final system design reviews, and the AP1000 design for GDA. As an example, in response to questions, Westinghouse stated that the design pressure of the CCS had been specifically raised from 150 to 200 psig (10.34 to 13.79 barg) to prevent unnecessary actuation of safety relief valves during maintenance, (by raising the valve set points).

689 Westinghouse has stated that they consider a major safety benefit of the CCS was the use of two segregated cooling towers within the Service Water System as the ultimate heat sink, thus avoiding the need to interface with sea water, (with the possibility of blockages due to marine effects). It should be recognised that the AP1000 may use sea water for condenser cooling to support the conventional island power generation equipment, but I am satisfied that the selection of air based cooling for the SWS has effectively eliminated maritime external hazards by design.

690 I have also questioned Westinghouse on the design of the CCS to account for water hammer phenomena. They have responded that the CCS has been designed taking into account OEF from utilities, and includes features to mitigate this effect such as selection of valve operation times and a high point surge tank. I am satisfied that Westinghouse has recognised this phenomenon within their design, and have not pursued this line of enquiry further within GDA.

691 I have also questioned Westinghouse regarding the provision of CCS make-up. They have responded that this is effected via the Demineralised Water Transfer and Storage System which feeds into the surge tanks, associated with each CCS train. Each surge tank itself is sized to accommodate a maximum leak rate either into or out of the system at 11400 litres per hour for 30 minutes; although the Demineralised Water Transfer and

Storage System is capable of higher make-up rates. Westinghouse has also stated that the AP1000 design surge tank and make-up design is the common approach in the US. I am satisfied with this response and the system design from a GDA perspective.

692 I am aware that the original design of the AP1000 used a common discharge and suction header for both trains of the SFS. A design change was then instigated at the request of utilities to provide separate discharge and suction headers to the spent fuel pool, which I agree to be in line with good engineering practice. I consider it to be an Assessment Finding (**AF-AP1000-ME-35**) that this is fully reflected in all necessary design and safety documentation.

693 I conclude, I am satisfied with the description and Mechanical Engineering designs of the main nuclear island cooling trains from a GDA perspective against SAPs EHT.1, EHT.3 and EDR.1.

4.16.1.3 Heat Exchanger Designs

694 I have also assessed the general designs of heat exchangers used within the AP1000 design, in terms of their design pedigree, Operational Experience Feedback, and maintenance requirements / practicability. I have specifically assessed the Mechanical Engineering features and system design associated with the single Passive Residual Heat Removal Heat Exchanger. This is a specific feature of the AP1000 design, and is used as a Safety System to remove decay heat from the reactor core under defined fault scenarios.

695 I questioned Westinghouse on the Mechanical Engineering design of selected heat exchangers within the AP1000 facility, (TQ-AP1000-199, TQ-AP1000-736, Ref. 10). Westinghouse responded with the following information:

- Reactor Coolant Pump Heat Exchanger – standard shell and tube design.
- PRHR HX – ‘C’ tubes connected to channel heads.
- Normal Residual Heat Removal Heat Exchangers – standard shell and tube design.
- Spent Fuel Pool Heat Exchangers – plate and frame design.

696 I questioned Westinghouse on the selection and design of the plate and frame heat exchangers, on the basis of my initial thoughts that these are less robust than shell and tube designs. This subject was discussed during technical meetings where Westinghouse provided information on the operating experience and application of plate and frame heat exchangers, as proposed within the AP1000 design for specified heat exchange requirements. Information was also provided in response to my technical query specifically addressing this line of enquiry, (TQ-AP1000-391, Ref. 10).

697 Westinghouse stated that plate and frame heat exchangers have been selected for the AP1000 for low pressure and low temperature applications, they are extensively used in the nuclear industry by several utilities, and that they would compile a report on OEF and applications for Plate (and frame) Heat Exchangers (PHE) for ND and the utilities; (this is discussed below).

698 Westinghouse described some of the disadvantages of use of a PHE, namely:

- Low pressure and temperature application only.
- Potential for blockage due to small plate separation, which requires the provision of high quality fluids.

- Potential for leakage.
- Potential for fouling.

699 They explained that the main protection against corrosion is afforded by correct material selection, for the plates and the associated gaskets. Protection against bio-fouling is provided by upstream filtration, chemical treatment of the fluid, adequate frequency of mechanical and chemical cleaning, and back-flushing as necessary. Westinghouse stated that for the GDA AP1000 all the systems are closed loop systems, and there was therefore no requirement and hence provision for fixed system chemical cleaning. Indications of clogging and / or fouling is provided by measurement of decreased thermal performance, and / or increased pressure drop in either of the media. Both of these phenomena are detectable and need to be monitored to optimise the maintenance programme; (the AP1000 design provides provision for this).

700 Westinghouse stated that leakage could occur within / from the PHEs due to the following:

- Damaged gaskets.
- Excessive corrosion.
- Physical plate damage.
- Trapped objects between plates.
- Water hammer effects.
- Other transient operating conditions.

These are protected against in the AP1000 design by adequate material selection, adequate system design, and adequate maintenance.

701 The gaskets on each plate have a limited service life dependent on service conditions, and they predicted an expected service life of between 8~10 years depending on conditions. The AP1000 PHE design allows for 10% over-surfacing, and each frame can receive an additional 20% number of plates to be added. Austenitic stainless steel is also selected as a standard material for the plate design.

702 Westinghouse has now produced the report to summarise their engineering justification for the use of plate and frame heat exchangers, 'Use of Plate Heat Exchangers (PHE) in Westinghouse AP1000', (Ref. 19). This document discusses the following aspects pertinent to the use of PHEs in the AP1000 design:

- General description, including advantages and disadvantages of usage:
 - i) Advantages of very good heat transfer due to plate design.
 - ii) Advantages of compact design.
 - iii) Advantages of good temperature characteristics afforded by pure counter-current flow.
 - iv) Advantages of low sedimentation build up due to induced turbulent flow.
 - v) Advantages of ease of maintenance, since individual plates can be removed in situ.
 - vi) Disadvantages of low temperature / pressure application.
 - vii) Disadvantages of leakage potential through gaskets.

- viii) Disadvantages of bio-fouling potential, requiring EMIT.
- ix) Disadvantages of plugging, requiring straining / filtering equipment.
- x) High pressure drop requiring appropriate system design.
- PHE applications in nuclear power plants:
 - i) Used for component cooling water / service water interface extensively in the EDF fleet.
 - ii) Used in Swedish NPPs, including for spent fuel pool cooling application.
 - iii) Used at a number of US NPPs.
- Operating Experience Feedback, covering:
 - i) Sedimentation.
 - ii) Crystallisation.
 - iii) Corrosion.
 - iv) Bio-fouling.
 - v) Leakage, prevented by adequate material selection, adequate system design, and adequate EMIT regime.
- Use of PHEs in the AP1000:
 - i) Used for Component Cooling Water System to Service Water System heat exchange.
 - ii) Used for turbine building closed cooling water system.
 - iii) Used for Spent Fuel Pool Cooling heat exchange.
 - iv) Used for liquid rad. Waste system heat exchange.
- Maintenance programmes:
 - i) Cleaning, with experience of complete cleaning operation for one heat exchanger completed within 24 hours.
 - ii) Gasket replacement can be undertaken in a similar timeframe as for plate cleaning, with an estimated gasket life of 8 to 10 years.
 - iii) Full plate / gasket replacement can be achieved over circa 56 hours (excluding the time for refurbishment of the removed plates at the manufacturer).
 - iv) Individual plates can be removed and replaced as necessary.

703 In summary, I consider that Westinghouse has provided an adequate justification for the use of PHEs within the AP1000 design from a Mechanical Engineering perspective in respect of SAP EDR.1. They have recognised both the advantages and disadvantages of usage of this heat exchange technology, and have provided evidence regarding the pedigree of the design principle, and have presented and analysed OEF. I also place value on the flexibility afforded by the use of PHEs, in terms of the ability to replace individual plates and gaskets, and even the complete heat exchanger, in relatively short timescales. I now accept the use of PHEs within the AP1000 design.

4.16.1.4 Passive Residual Heat Exchanger

704 In response to a request for clarification and background explanations, Westinghouse provided information on the purpose of the single Passive Residual Heat Removal Heat Exchanger, PRHR HX, focussing on the selection of a single heat exchanger for this application. This was in response to my technical query (TQ-AP1000-200, Ref. 10), and technical meeting discussions.

705 The PRHR HX is associated with the passive core cooling system of the AP1000. The PRHR HX is normally isolated from the appropriate Steam Generator RCS leg by two parallel, normally closed, fail open Air Operated Valves (AOVs). The PRHR HX can also be isolated by use of a single motor operated valve which is normally open (see Figure 5).

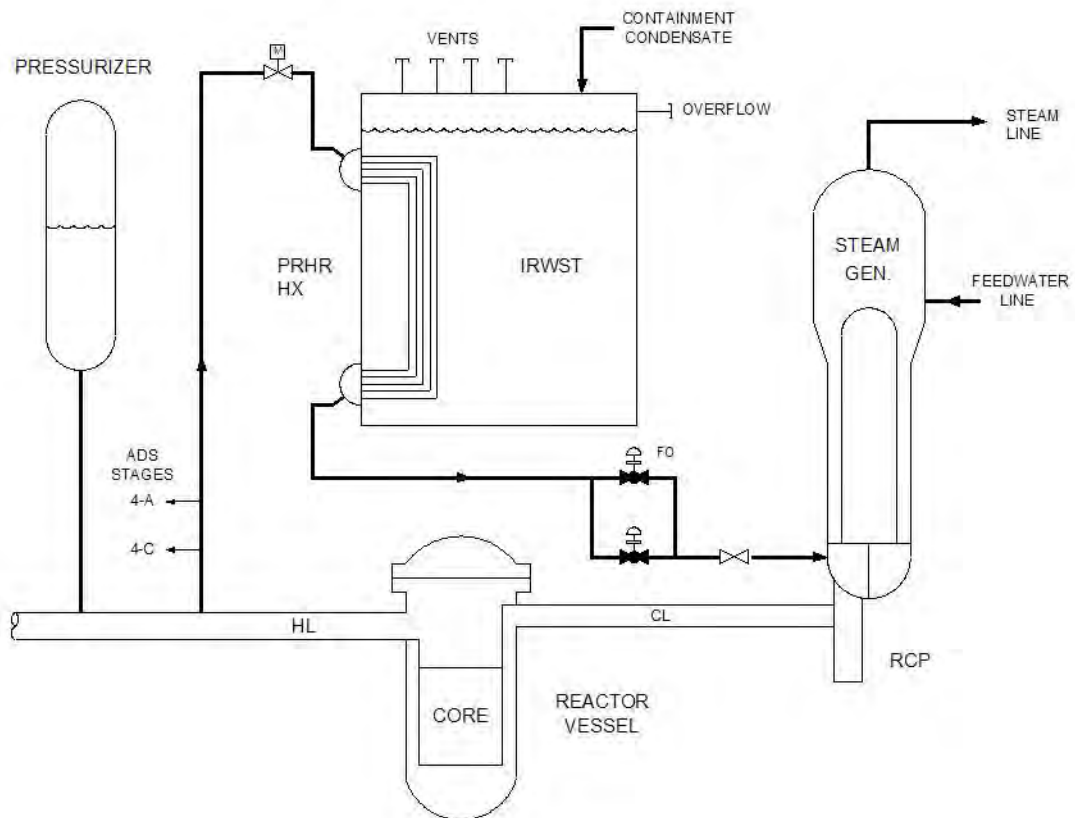


Figure 5

Passive Residual Heat Exchanger – Schematic Flow Diagram

706 The PRHR HX is situated within the IRWST, which provides for circa 2 hours of heat absorption, prior to saturation (boiling). Steaming is condensed by the Passive Containment System and then returned to the IRWST by guttering / channels etc.

707 Westinghouse explained that the return cold leg of the PRHR HX is connected to the steam generator channel head rather than the steam generator return cold leg to avoid problems due to RCP pressures and unpredictable flows.

708 The PRHR HX design comprises a bundle of Inconel 690 'C' tubes using standard flat tube sheets in line with standard steam generator technology.

709 The primary purpose of the PRHR HX is to provide passive heat removal for non-LOCA accidents (intact circuit faults), caused by Loss of Offsite Power, Secondary Side pipe

breaks (feedwater and steam lines), and steam generator tube ruptures. The PRHR HX also plays a limited role in small LOCAs to reduce the RCS pressure.

- 710 Westinghouse stated that the PRHR HX is designed to withstand any credible single failure: an active valve failing to open is designed out by provision of parallel AOVs; spurious closure of the Motor Operated Valve is eliminated by removal of power during EMIT, Tech Spec administrative control, and provision of redundant position indicators. Miss-positioning of manual valves is not considered credible due to position locking, plus limit switch position monitoring and alarms. Line blockage is not considered credible by Westinghouse due to the large pipe bore (14 inch). I consider these claims to be reasonable from a Mechanical Engineering perspective.
- 711 In terms of possible provision of two PRHR HXs, Westinghouse stated this was not considered practicable due to space constraints; the single PRHR HX is connected to the single steam generator leg which is positioned close to the IRWST. Furthermore, due to space constraints they do not consider it practicable to connect two sets of pipes to one hot leg and one steam generator. Westinghouse also stated that provision of two heat exchangers could make a steam line accident worse due to excessive RCS cooldown.
- 712 Westinghouse stated that it is possible to remove the PRHR HX during the life of the plant, for maintenance and renewal. Westinghouse also stated they did not consider it to be practicable to provide two MOVs, primarily due to space constraints, and the large sizes of the valves.
- 713 I am aware that Westinghouse has identified the need for a design change, in order to shut down the reactor in the event of spurious activation of one of the two PRHR HX AOVs. This is reported in Section 4.8 of this document.
- 714 In summary, and subject to the implementation of the identified design change, I am now satisfied with the design of the PRHR HX and associated system, from a Mechanical Engineering GDA perspective against SAP EDR.1.

4.16.2 Findings

AF-AP1000-ME-33: *The licensee shall ensure that the RNS / SFP heat transfer calculations are reviewed against the site specific predicted temperatures / conditions, to ensure that the design remains adequate. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-34: *The licensee shall assess the practicability of inspecting and / or replacing detrimentally affected sections of the CCS in respect of corrosion, and implement any necessary ALARP improvements which are identified. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-35: *I am aware that the original design or the AP1000 used a common discharge and suction header for both trains of the SFS. A design change was then instigated to provide separate discharge and suction headers to the spent fuel pool. The licensee shall ensure that this design change is fully reflected in all necessary design and safety documentation. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive*

commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

4.17 Diesel Generators

715 Diesel generators are traditionally designated as part of a safety system. They typically provide a diverse means of providing AC power to support the operation of components that are important to safety. They are accordingly assigned with the appropriate safety function categorisation and equipment classification.

- Safety Assessment Principle ESS.1 states ‘All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.’

716 My Step 3 assessment identified that Westinghouse had not initially assigned a safety claim on any of the diesel generators. This was due to Westinghouse’s claim on their Passive Safety System, which only required the support of a DC battery supply. Nevertheless, as part of Step 4 I progressed my assessment in this area to increase my understanding of their arguments and evidence in support of their philosophy.

4.17.1 Assessment

717 Following on from cross-cutting technical discussions during Step 3, Westinghouse has decided to proceed to develop a safety categorisation and classification philosophy that is more aligned to the UK regulatory expectations. As a consequence, and at the end of GDA, the diesel generator systems are now considered as items important to safety by Westinghouse, and are assigned with the appropriate safety function categorisation and equipment classification.

718 The AP1000 diesel generator systems comprise 2 standby diesels and 2 ancillary diesels. In addition the plant has provision to connect 2 additional transportable diesels as a temporary measure.

719 During discussion with Westinghouse they confirmed the assigned safety categorisation and classification for the AP1000 diesel generators are now as follows:

- Standby diesel generators Cat A Class 2.
- Ancillary diesel generators Cat B Class 2.

I have confirmed that this assigned safety categorisation and classification is reflected in the latest GDA documentation (Ref. 35), and this aspect is now aligned with my regulatory expectations.

720 The role, duty and safety functions of the diesel generators are described within EDCD EPS-GW-GL-700 Chapter 8.3, (Ref. 88).

721 The standby diesels have the following characteristics and functions:

- They are stand alone, self contained units furnished with their own support sub systems, they are water cooled and are air started.
- They provide a back-up source of electrical power to on-site equipment required to support:
 - i) Decay heat removal during reduced reactor coolant system inventory and mid-loop scenarios.

ii) Investment protection for short term availability controls and the design reliability assurance program.

- They have an individual air receiver that has the capacity to attempt to start a generator 3 times, which is normal practice for the US plants.
- They power the IDS class 1E battery chargers and transformers.
- They provide for the safety related loads, for example service feedwater, component cooling water, spent fuel cooling and residual heat removal systems.
- They are able to reach speed, voltage for electric loads within 2 mins of a start signal.
- They are located within a single building, which is a seismic category II structure, the building is separated into 2 areas by a fire rated wall, (anchorage details were also seismic category II qualified).

722 The ancillary diesels have the following characteristics and functions:

- They provide AC power for Class 1E post accident monitoring, C&I room ventilation, pump power to refill the PCS water storage tank on the top of the shield building and the spent fuel pool when all other sources of power are not available.
- They do not support the first 72 hours of loss of AC power supply.
- They have a manual start facility but require the aid of batteries.
- They are located within the annex building, which is a seismic category II structure but with no room segregation, (anchorage details were also seismic category II qualified).

723 Westinghouse stated that Operating Experience was captured within a discreet section of the diesel generator specification (Ref. 38) and is a suppliers' contract deliverable. However, I consider that as the diesel generator systems have now been assigned important safety classifications, there is an increased level of importance for the equipment design to consider Operational Experience Feedback. I consider this to be an Assessment Finding (**AF-AP1000-ME-36**); a future licensee to generate evidence that the diesel generator systems that have now been assigned as being important to safety have adequately considered Operational Experience Feedback.

724 As part of my assessment I was interested in understanding how Westinghouse are considering the amendment to the Motor Fuel (Composition and Content) Regulations 1999, which is to be implemented under EU Directive 2009/30/EC. The amendment is concerned with implementing more stringent control of fuel parameters, which have an environmental impact. I consider it to be of particular interest to understand the impact of the increased use of biofuels and the consequential effects on diesel generators.

725 Westinghouse's response to TQ-AP1000-1002 (Ref.10) failed to answer the question posed on the amendment to the Motor Fuel (Composition and Content) Regulations 1999, which is to be implemented under EU Directive 2009/30/EC. I consider this to be an Assessment Finding (**AF-AP1000-ME-37**); a future licensee to generate arguments and evidence on how the proposed diesel generator designs consider and comply with the revised fuel regulations.

726 The response to TQ-AP1000-1002 also described and provided evidence of the design process considering the effects of contaminated fuel and fuel aging, which has resulted in the system design incorporating several features to manage the design constraint. I consider this part of the response to be acceptable.

4.17.2 Findings

AF-AP1000-ME-36: *The licensee shall generate evidence that the diesel generator systems that have now been assigned as being important to safety have adequately considered Operational Experience Feedback in terms of their design and EMIT requirements. Target Milestone – install diesel generators complete as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-37: *Westinghouse's response to TQ-AP1000-1002 (Ref.10) failed to answer the question posed on the amendment to the Motor Fuel (Composition and Content) Regulations 1999, which is to be implemented under EU Directive 2009/30/EC. The licensee shall generate arguments and evidence to ensure the proposed diesel generator designs consider and comply with the revised fuel regulations. Target Milestone – install diesel generators complete as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.18 Fuel Handling

727 I have undertaken a limited assessment of the receipt of new fuel into the AP1000 NPP, and have also looked at the mechanical equipment for handling spent fuel within the plant. This general topic area is also covered under the subject of cranes, reported elsewhere in this report.

728 I decided to review the anti-siphoning features of the spent fuel pool, since this is an important consideration to ensure that the spent fuel pool maintains an adequate coverage of treated water to provide cooling and shielding for the spent fuel.

729 I consider the following Safety Assessment Principle to be relevant to this aspect:

- Safety Assessment principle EDR.1 (Ref. 4) states 'Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.'

4.18.1 Assessment

4.18.1.1 Mechanical Equipment

730 Westinghouse has described the mechanical equipment associated with the receipt of new fuel for the AP1000 (TQ-AP1000-611, Ref. 10), noting that there are no design features which support the handling of reprocessed fuel or mixed oxide fuel. In particular Westinghouse has stated that no scaffolding is required as part of the process to inspect new fuel. Once inspected new fuel is then placed inside the new fuel storage area, using the new fuel hoist and new fuel handling tool. The fuel is subsequently moved into the spent fuel pool, via the new fuel elevator equipment.

731 I have questioned Westinghouse in respect of the possibility of inadvertently handling spent fuel using the new fuel handling tool. In response (TQ-AP1000-1216, Ref. 10) they have clarified that the spent fuel is handled by the dedicated long tool, which is circa 10.5m in length, and whose use ensures that the fuel retains an adequate coverage of water for shielding and cooling. The new fuel handling tool is much shorter in length, being circa 0.9m long. The spent fuel hoist down limit is also interlocked to prevent the

hook becoming wetted (i.e. contacting pool water), and hence if the small tool was inadvertently attached, it would still not be able to connect to spent fuel. In addition, both tools are manually operated from the top, and so use of the small tool for handling spent fuel is not considered credible. I agree with this conclusion since the top of the small tool would have to be significantly under water to interface with the spent FAs.

732 In response to questioning, Westinghouse has described the mechanical handling equipment used to transfer new and spent fuel between the spent fuel pool, and the reactor pool (TQ-AP1000-734, Ref. 10). They have described the maintainability features associated with this equipment, and also the capability for manual recovery in the event of equipment failure. Westinghouse has stated that the design improvements associated with this equipment were the result of years of operating experience, and liaison between operators and equipment suppliers.

733 In summary, I consider the AP1000 fuel handling equipment to represent mature technology, and I have not identified any issues of concern from the descriptions provided by Westinghouse. I am therefore content with the proposed designs from a GDA perspective against SAP EDR.1.

4.18.1.2 Spent Fuel Pool Connections

734 I have reviewed the spent fuel pool mechanical design features, including anti-siphoning arrangements, as part of my Step 4 assessment, TQ-AP1000-1264 (Ref. 10). The anti-siphoning design arrangements are important to prevent loss of water from the pool in the event of leaks or breaks within the attached pipework systems.

735 The penetrations of the spent fuel pool were summarised as follows:

- Single RNS pump suction line.
- Single RNS discharge line (with anti-siphon hole).
- Two Spent Fuel Cooling (SFS) suction lines.
- Two Spent Fuel Cooling (SFS) discharge lines (with anti-siphon holes).

736 The suction lines are simple penetrations in the side of the pool, without pipework extending into the body of the pool. The discharge lines comprise pipework with a 'swan neck' feature into the pool, which have a 25mm nominal diameter anti-siphoning hole at the top, which Westinghouse explained was a standard feature for their spent fuel pool design. Through discussion Westinghouse did not identify any credible failure mechanism associated with this anti-siphoning hole. The two SFS lines are segregated, located in separate fire zones and powered by separate electrical supplies, which has been a design change at the request of the European utilities.

737 There are two pool surface skimmers, which act as filters for surface particulate, and which are each connected to a separate SFS suction line, to generate the necessary suction flow. Westinghouse stated that this arrangement is seen as an improvement over previous designs, since it obviated the need for separate skimmer suction and discharge pipework.

738 The spent fuel pool is filled from the Demineralised Water System (DWS), with approximately 2 weeks duration between fills, during which the pool level falls approximately 180mm. The level is measured, with trending to notice abnormalities, and with alarm set-points chosen to allow sufficient time for remedial action.

- 739 Westinghouse described the hazard of pool overflow, with spill-over provision into the Cask Loading Pit (which is maintained at ~300 mm below pool level), followed by Cask Loading Pit spill-over to the Cask Washdown Pit (which is normally empty).
- 740 Westinghouse stated that for spent fuel in the fuel racks, operator doses are considered insignificant. For spent fuel lifted to the maximum permissible height in the pool, the dose rate is 25 microSv per hour for an operator on the fuel handling machine.
- 741 The spent fuel pool purification and demineralisation systems provide two full pool cycles in 24 hours. There is also continuous air sampling while moving fuel to evaluate airborne activity. Westinghouse also explained that spent fuel pool temperatures are minimised by design, (normal maximum as ~49°C).
- 742 During fuel movements the minimum clearance from the spent fuel assembly to the top of the racks is 228mm, to provide margin against mechanical interference.
- 743 Westinghouse stated that the spent fuel pool design is consistent with the AP1000 maintenance guidelines, and manufacturers' recommendations, and has been simplified by elimination of separate skimmer pumping circuits. The system also includes the capability to use the RNS circuit for pool cooling, giving additional capability for spent fuel cooling system maintenance.
- 744 The safety functions associated with the spent fuel pool systems, in line with UK guidance, are as follows:
- Category A functions
 - i) Remove decay heat from the spent fuel pool.
 - ii) Maintaining spent fuel pool integrity.
 - iii) Controlling pool reactivity.
- 745 Overall, I consider Westinghouse has described an adequate design, and I am now satisfied that appropriate safety function categorisations have now been applied. I am now satisfied in this area from a GDA Mechanical Engineering perspective against SAP EDR.1.

4.18.2 Findings

- 746 I have not identified any findings covering this area.

4.19 Drains and IRWST Sump Screens

- 747 I have undertaken a targeted assessment of the Mechanical Engineering features of drains and filters / screens used within the AP1000 design. I consider the following Safety Assessment Principle to be applicable to this assessment area.

- Safety Assessment Principle EQU.1 (Ref. 4) states 'Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.'

4.19.1 Assessment

4.19.1.1 AP1000 Drainage Systems

- 748 I targeted my assessment on the AP1000 drain systems to ensure adequate arrangements are contained within the NNP design to manage process effluent wastes and their associated radioactive and contamination hazards.
- 749 Westinghouse provided information and an explanation of the Liquid Radwaste System (WLS), the Radioactive Waste Drain System (WRS – covering radioactive drains outside of containment), and the Waste Water System (WWS).
- 750 The primary safety functions of these drain systems are as follows:
- WLS – to receive and process radioactive floor drains, and to mitigate a Design Basis Accident.
 - WRS – to collect radioactive drainage.
 - WWS – to prevent release of water if it becomes contaminated.
- 751 Westinghouse clarified the WLS filter as being safety category B, class 3 equipment, and as being a nuclear standard filter design as used in other similar applications, which is in line with my expectations.
- 752 In response to questioning, Westinghouse stated:
- Active and non active sumps are adequately separated to prevent the draining of active liquor into a non active drain.
 - All containment active sumps incorporate high and low level detection, allowing automatic pump start up on a high level indication and their tripping on a low level indication.
 - All drains lines are fabricated from welded stainless steel, except where flanges are necessary for the incorporation of valves and pumps etc, which is to support EMIT.
 - The technology for sump monitoring is under development, and they were working to standardise the design, with the solution either being radar or ultrasonic. The sumps are monitored with one instrument, with one pump starting on a high signal, and a second pump starting on a high-high signal. Westinghouse described the use of deep sumps (i.e. small area and deep for a given total volume), and explained they provide a higher depth variation for a given volume variation, and provided an increase in sensitivity.
 - The AP1000 design provides complete segregation of radioactive from non-radioactive drains; and of chemical from non-chemical drains.
- 753 Drain lines in the Radioactive Waste Drain System (WRS) are sized such that the drain is able to accommodate the maximum anticipated daily flow rate of 120 US gallons per minute (gpm) (454 litres per minute), which corresponds to the flushing of the drains using the Solid Radwaste System (WSS) resin transfer line and gives consideration to the static head and the pipework pressure drop.
- 754 In abnormal conditions, the maximum flow rate is 250 gpm (946 litres per minute), corresponding to the stream of two fire-fighting hoses in the case of a fire. This flow rate is accommodated by all of the 138 WRS drains, except for 11, which are located at elevation 66' 6" in the radiological controlled areas of the Auxiliary Building. At this elevation, some of the rooms will be partially flooded during abnormal operation conditions before their drains can accommodate the 250 gpm (946 litres per minute).

- 755 Westinghouse claimed the flooding in this scenario to be acceptable. I have not pursued this aspect during my assessment since this is considered to be outside the discipline of Mechanical Engineering, but I have advised my Internal Hazards colleague as appropriate.
- 756 Westinghouse described the incorporation of Operational Experience Feedback into their designs, specifically with inlet drains being kept submerged to prevent back gassing, covers to keep out debris, and the provision of redundant pumps to prevent overflow.
- 757 In response to questions on clarifying why the WLS sump pumps are positioned submerged within their drain tanks and how EMIT is carried out, Westinghouse stated that spatial constraints and Net Positive Suction Head (NPSH) requirements require the pumps to be submerged within the drain tanks for normal operations. The pumps are also required to be of a submerged design to allow the pumping of containment water, in a flood scenario following an event.
- 758 Concerning EMIT and access, Westinghouse has stated the Reactor Coolant Drain Tank (RCDT) has a demineralised water connection and a drain line. This allows the RCDT to be filled with demineralised water to decontaminate the item and tank; with a hose taking the washings from the drain connection on the tank to a local room sump.
- 759 I consider this to be another example of space constraints dictating the selected design choice, which is not of the first design choice, but which I consider to be acceptable based on a proportional consideration of hazard and risk.
- 760 Westinghouse agreed to provide the arguments and justification for the choice of a 1/100 minimum slope for all drain lines to maintain velocities and thus prevent particulate settling. They subsequently provided the following information:
- The design standard for 'falls' on drain pipework follows the International Plumbing Code, Uniform Plumbing Code and the BOCA National Plumbing Code, which requires a minimum slope of 1/8 inch per foot (1 m/100 m) for drain lines 4 inch to 8 inch in size.
 - Plumbing codes are typically used as the bases for slopes in nuclear drainage systems.
 - Operating Experience Feedback has not documented any issues with the use of this design criteria.
- 761 I consider the arguments and justification to be generally aligned with my expectations, and I am satisfied from a GDA perspective against SAP EQU.1.

4.19.1.2 IRWST Screens

- 762 I decided to assess the IRWST recirculation screens since these play an important part in the operation of the Passive Core Cooling System, to ensure that the flow of water is not impeded by the build of debris. Although such screens are a standard feature of PWR NPPs, to provide the water for long term core cooling in the event of a LOCA, I considered that the passive nature of the AP1000 safety systems, and the associated gravitational driving heads, placed a greater reliance on screen performance. I had also become aware during Step 4 that some design changes had been proposed in this area.
- 763 Westinghouse has described the IRWST and containment recirculation screens, and associated design requirements, TQ-AP1000-1266 (Ref.10). An important part of the design requirement has been the establishment of the debris loading predictions. The debris inside containment comprises:

- Latent debris, (particles and fibres).
- Zone of Influence Coatings (ZOI) - within the ZOI of a LOCA coatings are assumed to fail in a worst case manner as fine particles.
- Chemical effects, leading to precipitated chemical products.

764 The latent debris has been estimated from walk-downs covering 34 plants, and then conservative values assumed in the subsequent analysis. Westinghouse estimated that 5% of this latent debris would consist of fibre material, and the remaining 95% as particulate.

765 Westinghouse also provided detail on how the ZOI was established relative to a LOCA location, and then described the type of coatings present within the AP1000 design.

766 The following aspects have been incorporated within the AP1000 design in recognition of the potential of blocking recirculation of the passive core cooling system, following a LOCA:

- Very low debris generation / transport, with no fibrous material generated by a LOCA.
- Enhanced debris settling, due to deep flood up levels and low flow velocities; plus delays before recirculation (allowing settling of debris).
- Protective plates above screens, helping to prevent particulate transport to the screens.
- Provision of generous screen surface area.
- Reduced use of coatings within containment.

767 The IRWST screens comprise large vertical fabrications, containing a large number of rectangular section pockets, where water flows through the screen to the back, where there is a connection to the passive core cooling system pipework. The screen is designed to minimise the pressure drop across itself due to the flow of water, and the lowest surface is circa 150mm above the IRWST floor to avoid blocking by settled debris.

768 Westinghouse described the comprehensive testing regime they had undertaken to substantiate the screen design, comprising simulation of typical debris and generation of large flows through screens to measure the associated pressure drops. Westinghouse stated that during this testing it had been very difficult to mobilise the debris in the water, which had required significant manual and motorised agitation, and which they considered evidence of the tendency of the suspended material to settle quickly; this was positive evidence in terms of operation of the passive core cooling system.

769 Westinghouse explained that the tests had been very conservative, but unfortunately the last test had been overly so in their opinion, and a significant pressure drop had occurred, causing the test to fail the pre-set criteria. This had led to difficulties with the US NRC; and as a result of this the AP1000 design has now been enhanced by the addition of a cross connection between the two specified IRWST screens, plus the provision of a third screen in the cross connection line. Westinghouse also stated that the PXS recirculation squib valves and the IRWST injection squib valves are qualified for operation under water.

770 Westinghouse claimed that they are now confident that following this design modification, the screen design and associated system would be acceptable to the US NRC. I consider it to be an Assessment Finding (**AF-AP1000-ME-38**) that this design change,

incorporating adequate consideration of any further comments from the US NRC, is incorporated into the AP1000 design.

- 771 In response to my questions, Westinghouse stated that any corrosion which would be generated over the life of the plant had been accounted for in the conservative estimate of debris loadings from the plant walk-downs. They also commented that although debris loadings had been estimated from walk-downs, there was no associated permissible value or limit associated with this parameter, since plants were intended to be kept as clean as practicable; which I consider to be rational and reasonable.
- 772 In response to my questions, Westinghouse stated that precise water levels for the passive core cooling system are not that significant, and as such the design is not sensitive to the civil build tolerances associated with the construction of the AP1000.
- 773 In respect of maintenance, Westinghouse stated that a visual inspection of the screens is a requirement every 24 months.
- 774 In summary, I am satisfied that Westinghouse has undertaken a comprehensive and rational design process, associated with the design of the screens and system, and this has been substantiated by a significant test programme. On this basis, I consider this aspect of the AP1000 design to be acceptable for GDA (subject to satisfactorily completion of the test programme) against SAP EQU.1.

4.19.2 Findings

AF-AP1000-ME-38: *Westinghouse stated that they are now confident that following the IRWST design modification, the screen design and associated system would be acceptable to the US NRC. The licensee shall ensure that this design change, incorporating adequate consideration of any further comments from the US NRC, has been incorporated into the AP1000 design and they report the satisfactory outcome of the test programme. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.20 Pond Stillages

- 775 I have undertaken a limited assessment of the fuel racks located with the spent fuel pool from a Mechanical Engineering perspective. I have undertaken this assessment to understand the safety functions associated with the fuel racks, and specifically any potential to damage spent fuel during mechanical handling operations. I have also sought to understand the pedigree of the design proposal, and the extent to which the design has benefitted from Operational Experience Feedback.
- 776 I consider the following Safety Assessment Principle to be relevant to this aspect:
- Safety Assessment principle EDR.1 (Ref. 4) states 'Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.'

4.20.1 Assessment

777 Westinghouse has described the Mechanical Engineering features associated with the spent fuel assembly storage racks within the spent fuel pool, (TQ-AP1000-995, Ref. 10). The fuel handling area is equipped with the following features to assist operators with placement and movement of FAs:

- PLC controlled fuel handling machine with precise automatic positioner.
- Digital position indication readout for the crane bridge, trolley and hoist.
- Automatic hoist speed reduction on FA entry into the rack.
- Remote underwater cameras to view FA rack insertion and removal.
- Fixed underwater lighting.
- Additional manual position indication of fuel storage locations.
- Water clarity maintained by two pool volume turnovers per day.

778 Westinghouse has also described the dropped load analyses undertaken as part of the fuel rack design, and the information provided correlates to that detailed in response to the associated regulatory observation concerning the spent fuel hoist design, (RO-AP1000-058, Ref. 11).

779 Westinghouse has stated that they have partnered with a specialist company for the design of the AP1000 fuel rack. They have stated that this company has been the principal supplier of fuel racks for US NPP application for the past circa 20 years, and also have a worldwide pedigree, including supply to Sizewell B.

780 In summary, I consider the AP1000 fuel racks located with the spent fuel pool to represent mature technology, and I have not identified any issues of concern from the information provided by Westinghouse. I am therefore content with the proposed designs from a GDA perspective against SAP EDR.1.

4.20.2 Findings

781 I have not identified any findings covering this area.

4.21 Radiation Waste Containers

782 At the start of the Step 4 assessment process I considered that there may have been some limited effort required in respect of Radiation Waste containers used within the Nuclear Power Plant.

4.21.1 Assessment

783 I have not identified any issues of a Mechanical Engineering nature with this Step 4 assessment worthy of consideration from a GDA perspective, and have liaised with the assessment discipline covering Waste and Decommissioning in coming to this conclusion.

4.21.2 Findings

784 I have not identified any findings covering this area.

4.22 Transportation Flasks

785 At the start of the Step 4 assessment process I considered that there may have been some limited effort required in respect of Transportation Flasks used within the Nuclear Power Plant.

4.22.1 Assessment

786 I do not consider that there are any features of the AP1000 which specifically constrain the development of transportation flasks for the UK, recognising that it will be a number of years from initial criticality before fuel is removed from the spent fuel pool.

787 I have not undertaken any further assessment in this area since I did not consider there were any matters of particular significance with respect to GDA.

4.22.2 Findings

788 I have not identified any findings covering this area.

4.23 Containment Doors and Hatches

789 I decided to assess the Mechanical Engineering features of the Equipment Hatches and Personnel Airlocks that provide access into the main containment for both equipment and personnel. These are part of the nuclear island main containment vessel, and have the safety function of preventing release of airborne activity following a Design Basis Accident. I consider the following Safety Assessment Principle to be relevant to this aspect.

- Safety Assessment principle ECV.1 (Ref. 4) states 'Radioactive substances should be contained and the generation of radioactive waste through the spread of contamination by leakage should be prevented.'

4.23.1 Assessment

790 Two Equipment Hatches are provided to allow passage of large equipment both into and out of the containment vessel, each provided with an electrically powered hoist. Each hatch is designed to ASME III, Division 1, Sub-section NE; with a design temperature and pressure of 149 degree C and 4.07 bar g respectively. The minimum service temperature is stated as 12 degree C, and the hatches have a design life of 60 years based on an operation frequency of once per year after initial plant operation.

791 The hatches incorporate a double seal arrangement, with the final material selection to be decided by the supplier, subject to the design specification (although EPDM is a likely choice). The double seal has a closed annular space, which is required to be tested in line with EMIT requirements, and associated test pipework was provided within the design. The seals have defined leakage criteria and radiation requirements, as well compression test requirements following thermal and radiation aging.

792 The hatches have a dedicated lifting system, and the hatch cover is effectively captured by the system such that (notwithstanding gross mechanical failure) it cannot fall inwards into the containment area.

-
- 793 Westinghouse described the Operational Experience Feedback, associated with the Equipment Hatch design, including the fact that the hatch cover moves circa 25mm away from the mating surface after unbolting to prevent seal damage, and the use of guide rails to position the cover during opening and closing operations.
- 794 Two Personnel Airlocks are incorporated into the containment vessel, to allow for ingress and egress of personnel during construction, plant operations, and outage periods. These airlocks extend outwards radially from the containment vessel shell. The airlock comprises a cylindrical tube, with doors at either end, each of which is operated via handwheels located on both the inside and outside of the door. The doors are mechanically interlocked such that only one door can be opened at the same time; albeit this can be bypassed during an outage to expedite passage of personnel, where access / egress is subject to administration control.
- 795 The airlocks are designed to ASME III, Division 1, Sub-section NE; with a design temperature and pressure of 149 degree C and 4.07 barg respectively. The minimum service temperature is stated as 12 degree C, and the hatches have a design life of 60 years based on an operation frequency of once per month after initial plant operation. Each door also has a double seal arrangement, with defined radiation and thermal aging test requirements, and leakage limitations, with provision to test the annular space by pressurisation.
- 796 Westinghouse described how Operational Experience Feedback had been incorporated into the design of the airlocks, summarised as follows:
- Gear boxes and shafts are located under the door for ease of maintenance.
 - Personnel can open the airlock doors from inside the containment Vessel using emergency tools.
 - Door stoppers are included to prevent driving mechanism damage.
 - Blind flanges are included for equalising valves for valve seat local leak testing.
- 797 Through discussion in the associated technical meeting in Pittsburgh, there was some uncertainty regarding the design life of the seals for both the Equipment Hatch and Personnel Airlock designs, and I decided to continue my assessment in this area through raising a technical query, (TQ-AP1000-1061, Ref. 10). In response to this query Westinghouse has stated that the seal material design life is not usually specified, but that circa 20 Japanese NPPs are successfully using these seals, however the seals are replaced at every outage. They have also stated that seals are subject to the following EMIT requirements:
- A seal tightness test is performed at least every two years.
 - Routine inspections of the 'as installed' seal should be performed between the periodic seal tightness tests.
 - The seal housing surface should also be inspected for signs of degradation.
- In view of the response from Westinghouse, I consider it to be an Assessment Finding (**AF-AP1000-ME-39**) that the seals for the Equipment Hatch and Personnel Airlock are changed at every outage, or an alternative EMIT strategy justified, and this is reflected in the EMIT documentation.
- 798 Notwithstanding this Assessment Finding, I am satisfied with the designs of the AP1000 containment doors and hatches from a Mechanical Engineering GDA perspective against SAP ECV.1.
-

4.23.2 Findings

AF-AP1000-ME-39: *The licensee shall ensure that the seals for the Equipment Hatch and Personnel Airlock are changed at every outage, or an alternative EMIT strategy justified, and this is reflected in the EMIT documentation. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.24 RPV Leak Detection System

799 I consider the reactor pressure vessel head seal arrangement has the important safety function of containing the primary circuit fluid, and consequently the AP1000 reactor pressure vessel leak detection system is an important mechanical design arrangement to ensure that leakage is identified, monitored, and effective action is taken as necessary in line with safety case parameters.

- Safety Assessment Principle ESS.3 states ‘Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions’.

800 As a consequence I targeted my assessment on the following aspects:

- Purpose, role and safety function.
- Evidence of equipment categorisation and classification.
- Examination, maintenance, inspection and testing regime.
- Consideration of relevant operational experience.

4.24.1 Assessment

801 This line of enquiry was initially pursued via a technical query, followed by discussion at a technical meeting in Pittsburgh. The Westinghouse description and justification was subsequently consolidated in the response to a further technical query raised following the meeting, (TQ-AP1000-1214, Ref. 10).

802 The RCS includes a reactor vessel flange leak-off detection subsystem to detect and monitor seal leakage. This system is now identified as providing a Category B safety function, and the equipment is designated as Class 2, in line with the revised AP1000 methodology. I am in agreement with this designation.

803 The RPV flange has two O-ring seals, each of which is monitored for leakage. The inner ring is the first to be monitored, initially via a resistance temperature detector; followed by measurement of coolant loss via the reactor coolant drain tank. After leakage past the first O-ring is detected the system is isolated (thus providing the containment safety function barrier), and then leakage past the second, outer O-ring is monitored, by the same detection and monitoring system.

804 The O-rings are specified to be changed at every outage, and the RPV only utilises one leak detection system, i.e. there is no redundancy / duplication.

805 Westinghouse has stated that this system was typical of that utilised within Westinghouse NPPs, although the overall reactor coolant pressure boundary leakage detection system

is an improvement over present operating plants, since it is capable of detecting a leakage rate of 1.9 litres per minute, compared to 3.8 litres per minute previously.

806 In terms of OEF, Westinghouse has stated that it has data for 55 O-ring failures for their designs of NPP; six have occurred since 2000, none since 2003. Out of the total, sixteen resulted in further penetration of the second, outer O-ring seal, resulting in an orderly plant shut down.

807 Westinghouse has also stated that any leakage past the outer O-ring would be classified as unidentified leakage, since it could not be accurately quantified, and hence lower operational limits would apply through the technical specifications, (Operating Rules). Furthermore, the containment sump monitors would complement the RPV leak detection system in this scenario.

808 I have reviewed the Operating Experience Feedback relating to the Sizewell B NPP in respect of the RPV leak detection system, specifically IRS report number 7643 (Ref. 83), 'Continued Reactor Operation with both Reactor Vessel Head 'O' Ring Seals Leaking due to Leak-Detection System Design Deficiencies and Lack of Boric Acid Leak Detection Programme'.

809 In summary this IRS report describes an event which occurred in May 2001, whereby the RPV head seal leak detection system initially indicated leakage from the inner head O-ring seal. The inner seal leak detection path was then isolated and the reactor continued operation in line with operating instructions. Later in the fuel cycle airborne activity levels, humidity, and sump levels in containment provided evidence of leakage from the Reactor Coolant System (RCS), but this always remained well within the Technical Specification limit for unidentified leakage.

810 Despite several containment entries, the source of the RCS leak was not identified, and in particular the thermocouple on the outer seal leak detection system indicated no sign of leakage. Subsequently, and due to increased levels of leakage in containment, plans for the reactor shutdown were brought forward, and following a detailed leak search the source of the problem was identified as a leak from the RPV head outer O-ring seal. The subsequent investigation revealed that the outer O-ring leak detection system would not reliably detect outer O-ring leakage when the reactor is at operating conditions. This outer O-ring leak detection system comprised a single hole in the flange to collect any fluid, and in this instance the actual leak site was at the opposite side of the RPV. Furthermore the high temperature of the RPV meant that any leakage would rapidly boil away, and not provide an indication of a leak by fluid collection by the outer O-ring leak detection system.

811 The IRS report concludes that although the inner O-ring leak detection is effective, the outer O-ring detection system has reduced reliability, and so if operating on the outer seal only, alternative indications such as containment activity, humidity, and drainage must also be used to detect outer seal failure.

812 The source of the leak itself was considered to be loose particle debris in the flange area which had occurred during maintenance activities, which is a known problem for RPV head closure sealing.

813 The consequence of a leak from the RPV is also boric acid crystal deposition, and associated corrosion of the low alloy steel of the RPV outer surfaces, which has been a significant problem for NPPs in the past.

814 On reviewing this information, I recognise that Westinghouse claim to have an established design system, with relevant OEF, and which has also been improved to provide greater measurement sensitivity. Nevertheless, the system described is generally

equivalent to that used at Sizewell B, and the IRS report has identified that the outer O-ring seal leak detection system is not reliable. On balance, I consider this to be an Assessment Finding (**AF-AP1000-ME-40**): the design of the RPV leak detection system should be reviewed against the findings of the IRS report, improvements identified as necessary, and justification provided as to why the design system is considered to be ALARP.

815 I also consider it to be an Assessment Finding (**AF-AP1000-ME-41**) that a future licensee reviews the safety case Operational Limits and Conditions to ensure that procedures are adequate to detect any passing of the outer RPV seal, such as measurements of containment activity, humidity, and drainage.

816 I also consider it to be an Assessment Finding (**AF-AP1000-ME-42**) that a future licensee should develop adequate EMIT procedures for the detection of leaks of boric acid generally within containment.

4.24.2 Findings

AF-AP1000-ME-40: *The licensee shall ensure that the design of the RPV leak detection system is reviewed against the findings of the IRS 7643 report, improvements identified as necessary, and justification provided as to why the design system is considered to be ALARP. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-41: *The licensee shall review the safety case Operational Limits and Conditions to ensure that procedures are adequate to detect any passing of the outer RPV seal, such as measurements of containment activity, humidity, and drainage. Target Milestone – fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

AF-AP1000-ME-42: *The licensee shall develop adequate EMIT procedures for the detection of leaks of boric acid generally within containment. Target Milestone – fuel on-site this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.25 Containment Penetrations and Vacuum Relief

817 I decided to assess the containment vacuum relief design, as an important design feature to prevent excessive vacuum being developed within the steel containment vessel under certain fault scenarios, and thus threatening the containment structural integrity. I had become aware during Step 4 that design changes had been proposed in this area.

- Safety Assessment Principle ESS.1 states 'All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.'

4.25.1 Assessment

- 818 Westinghouse described the vacuum relief system associated with the containment vessel, TQ-AP1000-1268 (Ref. 10). Westinghouse explained that the external pressure excursion is caused by a combination of faults / cooling events leading to condensation of the water vapour present within containment, thus generating the partial vacuum when compared to the external pressure.
- 819 The external design pressure for containment is 1.7 psig (11.7 kPa g), (i.e. -11.7 kPa g inside) against a normal pressure range of -0.2 psig (-1.38 kPa g) to 1.0 psig (6.9 kPa g) within containment, compared to the outside. Under the worst case transient modelled it is possible to generate a partial vacuum in excess of -0.8 psig (- 5.5 kPa g) as a Design Basis Event. This has led to the design of the pressure relief system which would actuate at -0.8 psig (-5.5 kPa g), and which comprises two parallel ASME Class 2 check valves inside containment, which are connected via a common header to two ASME Class 2 remote motor operated butterfly valves outside of containment, which operate on receipt of the appropriate safety signal on low containment pressure (or manual initiation). The motor operated valves are supplied from the safety batteries and the valve system effectively takes priority over containment isolation, in order to protect the containment vessel. However, the flow would be inwards until the pressure is equalised.
- 820 Only one outside motor operated valve and one inside check valve need to operate in order to provide vacuum relief. Therefore redundancy is provided for this safety system. The valves and piping are designed to ASME Section III, and all components are designed to satisfy seismic design criteria.
- 821 During the associated technical meeting I questioned Westinghouse on the initiating events which could lead to this scenario. Westinghouse stated that a number of scenarios had been modelled, including inadvertent actuation of the passive containment cooling system, inadvertent actuation of the active containment cooling system (fan coolers within containment), and station black out (loss of A.C. power). Westinghouse stated that the phenomena required an outside temperature of nominally < 0 degree C to occur, although the way the situation had been modelled was that they had sought to identify a worst case situation (including high winds to increase cooling), and determine the partial vacuum differential pressure accordingly, which had been assessed against the containment design pressure and used to specify the containment relief valve sizing.
- 822 I further questioned Westinghouse on the possibility of the containment ventilation system generating a partial vacuum to challenge containment integrity, necessitating the operation of the vacuum relief system. Westinghouse stated that both the extract and supply fans always operated at the same time, and so it would require a very significant mal-operation of the system to generate a threat, but by inspection of the fan curves it was possible to create a partial vacuum which could perhaps reach -0.7 psig (-4.8 kPa g), and thus possibly actuate the safety relief valves.
- 823 I consider that Westinghouse provided a good explanation of this partial vacuum phenomena associated with the containment vessel. They have designed an appropriate safety system to protect the vessel from the possibility of collapse, and I am satisfied against SAP ESS.1. Although the operation of this system would effectively breach containment, the flow of air would be inwards and I consider this to be the correct decision to terminate / mitigate this fault sequence. I consider it to be an Assessment Finding (**AF-AP1000-ME-43**) that this design change is fully incorporated into the AP1000 design.

4.25.2 Findings

AF-AP1000-ME-43: *The licensee shall ensure that the containment safety system to protect against the partial vacuum phenomenon has been fully incorporated into the AP1000 design and safety documentation. Target Milestone – Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.*

4.26 Steam Generator Feedwater System

824 I have reviewed the steam generator feedwater system during my Step 4 assessment, since this system has the safety function of providing cooling to the primary circuit under both normal and fault conditions.

- Safety Assessment Principle EHT.1 states 'Heat transport systems should be designed so that heat can be removed or added as required.'

4.26.1 Assessment

825 Westinghouse described the design for the feedwater supply systems for the two Steam Generators used within the AP1000 design, TQ-AP1000-1267 (Ref. 10). The overall system is divided into the Steam Generator System which is located in the auxiliary building and within containment, and the Feed Water System (FWS) which is located in the turbine building.

826 The Steam Generator System comprises the main feedwater supply lines, the start-up feedwater supply lines, the steam lines which lead to the turbine / condenser, and the steam generator blowdown system which connects to the lower portion of the steam generator and is used for chemistry control of the water residing in the steam generators. The isolation features within the main and start-up feedwater lines use check valves in series with pneumatically operated valves (using compressed nitrogen) for the main feedwater supply, and DC powered motorised valves for the start-up feedwater supplies. These are specifically designed as having passive features (Ref. 4), using stored energy to operate. Equipment is also provided to monitor feedwater temperature, pressure and flow as necessary. The Steam generator System is designed in accordance with ASME Section III.

827 The Feed Water System (FWS) provides the following functions:

- Supplies feedwater to the steam generators.
- Provides feedwater heating.
- Provides feedwater chemistry control.
- Provides decay heat removal under normal and fault situations.
- Provides a feedwater isolation function.

828 Westinghouse explained that by definition 'main feedwater' is feedwater flow that passes through the Main Feedwater Control Valves to the steam generators, and start-up feedwater is that which passed through Start-up Feedwater Control Valves to the steam generators, since there is interconnectivity within the FWS between main feedwater and

start-up feedwater supplies. The Feed Water System comprises pumps to provide flow and pressure, heaters, water supply tanks (Deaerator Storage tank and Condensate tank), and a chemistry conditioning system used before main feedwater flow can start. The start-up system is used during plant start-up, shutdown, low power operation (under 10% power), and for decay heat removal.

829 For the start-up feedwater portion of the FWS, water is supplied via the condensate tank, through two parallel pumps, through a common header to the individual steam generator lines, which contain the DC powered motorised isolation valves, check valves and a flow control valve. There is a cross connect to the main feedwater system within the FWS which allows a smooth changeover from the start-up to main feedwater supply systems.

830 The main feedwater system uses 3 x 50% fixed speed motor driven main / booster pumps. In response to questions, Westinghouse explained that fixed speed pumps have been selected on the basis of simplicity, to provide reliable operation, as opposed to variable speed pumps. The plant can be operated at 100% power with one pump train out of service for maintenance. Westinghouse stated that loss of one main feedwater pump train does not cause a plant trip, since the other redundant train can then be started by manual intervention. Westinghouse stated in clarification that this is an option, and not a safety requirement, since if the redundant train is under maintenance, then power would simply be reduced to 50%.

831 Westinghouse stated that the features of the AP1000 design allow for stable operation at start-up and better control at full load due to the combined use of the start-up and main feedwater lines due to the interconnectivity within the FWS. The use of the Deaerator Storage Tank to supply the main feedwater also provides a large Net Positive Suction Head for the pumps. The interconnection also allows use of the higher temperature Deaerator Storage Tank water for start-up (compared to the condensate tank water).

832 In response to questions, Westinghouse stated that the categorisation / classification for the main feedwater system is C3, and for the start-up feedwater system is A2, which is in line with my expectations, due to the greater safety significance of the latter. Westinghouse has recognised that the important features of the main feedwater duty system should attract an appropriate categorisation / classification. Overall I am satisfied with the explanations provided by Westinghouse for these systems, and have not identified any concerns for GDA against SAP EHT.1.

4.26.2 Findings

833 I have not identified any findings covering this area.

4.27 Chemical and Volume Control System

834 I have undertaken a limited assessment of the Chemical and Volume Control System (CVS), from a Mechanical Engineering perspective.

- Safety Assessment Principle ECS.2 (Ref. 4) states ‘Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regards to safety.’

4.27.1 Assessment

835 Westinghouse provided a description of the AP1000 Chemical and Volume Control System (CVS), which provides the major functions of:

- RCS purification.
- RCS inventory control.
- RCS chemistry control.
- Plant shutdown purification.

836 Westinghouse stated that the CVS adheres to the AP1000 design philosophy of simplification and standardization, and is designed for operating flexibility. In response to my questions, Westinghouse stated that simplification of the CVS has been made possible within the AP1000 design by design changes to other parts of the plant, e.g. the elimination of shaft seal pumps by the use of seal-less pumps. Westinghouse also stated that the design of the CVS as a high pressure system is not seen as a specific safety concern, since it is simply accommodated by the provision of appropriate high pressure designed equipment. I am content with this response from a Mechanical Engineering perspective.

837 Westinghouse stated that the AP1000 CVS is different to more traditional systems for the following reasons:

- No volume control tank (inventory additions occur via the auxiliary building make-up subsystem, and reductions through a separate let-down line exiting containment; also no continuous degassing of the reactor is required; (however, I understand that design modifications are underway in this area, with assessment led by the chemistry discipline).
- No requirements for significant system pressure changes.
- Use of gray rods simplifies the AP1000 CVS and reduces the number of make-up actuations.
- Number of valves and length of piping is greatly reduced because the purification loop does not run outside containment.

838 All CVS heat exchangers are shell and tube types, due to their high temperature and pressure duty requirements. Westinghouse has stated that the majority of components and functions in the CVS design are very similar to those used in the existing fleet. They are also undertaking an extensive review of OEF as applicable to the CVS, as part of their design process.

839 The CVS uses a software application for inventory control of the RCS, with typical operations involving daily measurement of the boron concentration of the RCS, which is used to control the position of a three way blend valve for boron control. In response to my questions, Westinghouse stated that the three way valve which connects to the boric acid batching tank, the boric acid storage tank, and the demineralised water supply fails safe, in the sense that it is spring loaded to fail to the boric acid storage tank position. In response to questions, Westinghouse stated that the system design is not specifically sensitive to failure of this three way valve, and failure of the valve would only lead to the need to reduce power, but it would not lead to the need for a reactor trip. I consider these responses reasonable and rational.

840 The safety functions and associated SSC classifications associated with the CVS (developed to date), in accordance with the latest methodology (aligned to the UK SAPs) are as follows:

- Category A safety functions:

- i) Maintaining the RCS pressure boundary integrity.
- ii) Maintaining the containment integrity.
- iii) Preventing unacceptable consequences due to spurious actuation.
- iv) Maintaining reactor coolant inventory.
- v) Control of subcritical core reactivity during normal and fault conditions.
- Category C function:
 - i) Controlling the level of radioactivity (within the purification loop and within the RCS).

841 Westinghouse described the following classified equipment associated with the CVS, in accordance with the UK methodology, including the following:

- Class 1
 - i) Purification inlet and return valves.
 - ii) Valves on the demineralised water supply line.
 - iii) Valves associated with containment penetration.
- Class 2
 - i) Make-up pumps.
 - ii) Boric Acid Storage Tank.
 - iii) Various valves.
- Class 3
 - i) Regenerative and letdown heat exchangers.
 - ii) Mixed bed and 'Cation' Bed demineralisers.
 - iii) Reactor Coolant and makeup Filters.

842 I consider that Westinghouse has described a rational and detailed design approach in respect of the CVS from a Mechanical Engineering perspective. However, at the end GDA, through liaison with my chemistry colleagues, I am aware there are design changes underway in this area, to ensure the system provides the correct functionality from a chemistry perspective. I have not identified any matters of concern from a Mechanical Engineering perspective for GDA against SAP ECS.2, although this conclusion is limited to the system as described, and the description of the design process.

4.27.2 Findings

843 I have not identified any findings covering this area.

4.28 Overseas Regulatory Interface

844 In accordance with its strategy, HSE collaborates with Overseas Regulators, both bilaterally and multinationally.

4.28.1 Bilateral collaboration:

845 HSE's Nuclear Directorate (ND) has formal information exchange arrangements to facilitate greater international co-operation with the Nuclear Safety Regulators in a number of key countries with civil nuclear power programmes. These include:

- the US NRC.
- the French Nuclear Regulator (ASN).
- the Finnish Regulator (STUK).

4.28.2 Multilateral collaboration:

846 ND collaborates through the work of the International Atomic Energy Agency and the OECD Nuclear Energy Agency (OECD-NEA). ND also represents the UK in the Multinational Design Evaluation Programme (MDEP) - a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. This helps to promote consistent nuclear safety assessment standards among different countries.

847 As an integral part of undertaking my Step 4 GDA process I have interacted with Overseas Regulators as part of the Multi Discipline Evaluation Programme (MDEP). Topics covered from a Mechanical Engineering prospective included the AP1000 squib valve designs and CRDMs. Participating MDEP Regulators included the US Nuclear Regulatory Commission (US NRC), Canada Nuclear Safety Commission (CNSC), and China Nuclear Safety Centre (NSC). This exercise has provided a useful exchange of information and has helped to guide my assessment in certain areas, the outcome of which is reported within the text of this document.

4.29 Interface with Other Regulators

848 As an integral part of undertaking my Step 4 GDA process I have interacted as considered necessary with the Environment Agency. A specific area of Mechanical Engineering where interaction was considered necessary was to progress the nuclear ventilation Regulatory Observation RO-AP1000- 043 (Ref. 11).

4.30 Other Health and Safety Legislation

849 I have considered conventional safety legislation in a general sense as part of my GDA assessment process, although I have not undertaken a systematic review in this respect, since I do not consider it appropriate for this scope and level of assessment. I have focussed my attention on the nuclear hazard, in line with the HSE-ND mission, to protect people and society from the hazards of the nuclear industry. Through my interactions with Westinghouse, I have reminded them of the requirement for any AP1000 constructed in the UK to comply with all relevant health and safety legislation, i.e. The Health and Safety at Work etc Act 1974 and its Relevant Statutory Provisions.

5 CONCLUSIONS

850 This report presents the findings of the Step 4 Mechanical Engineering assessment of the Westinghouse AP1000 reactor. Some of the observations identified within this report are of particular significance and will require resolution before HSE would agree to the commencement of nuclear safety related construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary these relate to:

- Engineering substantiation for the Mechanical Engineering (including pyrotechnic aspects) of the squib valve designs. The squib valves are fast acting valves used as part of the Passive Core Cooling System within the AP1000, and are novel designs which have been under development during GDA. Although the design development and associated prototype testing have made some good progress, due to the importance of these valves, the lack of finalised substantiation documentation, and associated justification shortfalls, I am not yet satisfied from a Mechanical Engineering perspective.
- Metrication of mechanical equipment to meet UK expectations. It is the UK Regulator's expectation that an AP1000 built in the UK will be a metric design. Although the AP1000 was originally conceived in imperial units, significant progress has been made in this area to meet the UK expectations. However, further work is still required, and a number of exceptions proposed by Westinghouse are either not acceptable, or require further definition and justification.
- Provision of adequate design features to enable the safe isolation and drainage of pipework for Examination, Maintenance, Inspection and Testing (EMIT) activities. Space is limited within the AP1000 design, and there are limited features to enable the safe isolation and drainage of pipework. Westinghouse has also proposed the use of pipe freezing as a routine activity. Further design work and justification is required in this area.

851 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for Mechanical Engineering. I consider that from a Mechanical Engineering view point, the Westinghouse AP1000 design is suitable for construction in the UK. However, this conclusion is subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.1 Key Findings from the Step 4 Assessment

5.1.1 Assessment Findings

852 I conclude that the following Assessment Findings listed in Annex 1 should be programmed during the forward programme of this reactor as normal regulatory business.

5.1.2 GDA Issues

853 I conclude that the GDA Issues listed in Annex 2 must be satisfactorily addressed before Consent can be granted for the commencement of nuclear island safety related construction.

6 REFERENCES

- 1 *GDA Step 4 Mechanical Engineering Assessment Plan for the Westinghouse AP1000*. HSE-ND Assessment Plan AR 09/045. November 2009. TRIM Ref: 2009/437146.
 - 2 *ND BMS. Assessment Process*. AST/001 Issue 4. HSE. April 2010. Available via www.hse.gov.uk/nuclear/operational/index.htm.
 - 3 Not used.
 - 4 *Safety Assessment Principles for Nuclear Facilities*. 2006 Edition Revision 1. HSE. www.hse.gov.uk/nuclear/saps/saps2006.pdf
 - 5 Not used.
 - 6 *Step 3 Mechanical Engineering Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/015. November 2009. TRIM Ref: 2009/287043.
 - 7 *ND BMS. Technical Assessment Guides*:
 - *Safety Systems*. T/AST/003 Issue 5. HSE. September 2009.
 - *ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)*. T/AST/005 Issue 4 - Revision 1. HSE. January 2009.
 - *Deterministic Safety Analysis and the use of Engineering Principles in Safety Assessment*. T/AST/006 Issue 3. HSE. July 2000.
 - *Maintenance, Inspection and Testing of Safety Systems, Safety Related Structures, and Components*. T/AST/009 Issue 1. HSE. November 1999.
 - *The Single Failure Criterion*. T/AST/011 Issue 1. HSE. October 2000.
 - *Integrity of metal Components and Structures*. T/AST/016 Issue 3. HSE. August 2008.
 - *Containment: Chemical Plants*. T/AST/021 Issue 1. HSE. February 2000.
 - *Ventilation*. T/AST/022 Issue 1. HSE. June 2000.
 - *Diversity, Redundancy, Segregation and Layout of Mechanical Plant*. T/AST/036, Issue 2. HSE. June 2009.
 - *Criticality Safety*. T/AST/041 Issue 2. HSE. March 2009.
 - *Nuclear Lifting Operations*. T/AST/056 Issue 1. HSE. July 2006.
 - *Design Safety Assurance*. T/AST/057 Issue 2. HSE. November 2010.Available via www.hse.gov.uk/nuclear/operational/index.htm.
 - 8 Not used.
 - 9 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels*. WENRA. January 2008. www.wenra.org.
 - 10 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 4*. HSE-ND. TRIM Ref: 2010/600721.
 - 11 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 4*. HSE-ND. TRIM Ref: 2010/600724.
 - 12 *Westinghouse AP1000 - Schedule of Regulatory Issues Raised during Step 4*. HSE-ND. TRIM Ref: 2010/600725.
-

-
- 13 *AP1000 Pre-construction Safety Report*. UKP-GW-GL-732 Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref: 2011/23759.
 - 14 *The Safe Isolation of Plant and Equipment*. HSG253. HSE. 2006. ISBN: 9780717661718. www.hse.gov.uk/pubns/priced/hsg253.pdf
 - 15 AP1000 Master Submission List. UKP-GW-GLX-001 Revision A. Westinghouse Electric Company LLC. February 2011. TRIM Ref: 2011/98980.
 - 16 *Regulatory Observation RO-AP100-38 and Regulatory Observation Action RO-AP1000-38.A1 – Metrication of the AP1000 for the UK*. Letter from ND to AP1000 Project Front Office. WEC70154R. March 2010. TRIM Ref: 2010/120974.
 - 17 *Westinghouse Updated Response to RO-AP1000-038, Metrication of the AP1000 for the UK: AP1000 Standard Plant Metrication*. Letter from ND to AP1000 Project Front Office. WEC70243R. 11 October 2010. TRIM Ref: 2010/491549.
 - 18 *AP1000 Standard Plant Metrication*. APP-GW-G1-011 Revision 3. Westinghouse Electric Company LLC. December 2010. TRIM Ref: 2011/79452.
 - 19 *Use of Plate Heat Exchangers (PHE) in Westinghouse AP1000 – Summary Report*. APP-ME30-VDR-001 Revision 0. Westinghouse Electric Company LLC. June 2010. TRIM Ref: 2011/93689.
 - 20 *Intermediate Design Review No. 07-34 KSB RCP Pressure Boundary Action Item #10*. Westinghouse Electric Company LLC. TRIM Ref: 2011/473790.
 - 21 *Design Specification. AP1000 Reactor Coolant Pump*. APP-MP01-M2-001 Revision 2. Westinghouse Electric Company LLC. August 2010. TRIM Ref: 2011/81474.
 - 22 *AP1000 Passive Core Cooling System (PXS) Valve (V018A/B) Test Specification*. APP-PXS T1-515 Revision 0. Westinghouse Electric Company LLC. 9 November 2009. TRIM Ref: 2011/209687.
 - 23 *Test Report for Prototype 8"-1707# N.o. Nozzle Check Valve, Westinghouse AP1000 Passive Core Cooling System (PXS-V016/17/A/B)*. MA 22982 Revision E. Curtis Wright Flow Control Company. September 2010. TRIM Ref: 2011/81899.
 - 24 *Design Change Proposal APP-GW-GEE-1954 Revision A. AP1000 Test Connection Modification for CMT Outlet Nozzle Check Valves PXS-V016A/B & V017A/B*. Westinghouse Electric Company LLC. July 2010. TRIM Ref: 2011/79498.
 - 25 *3" Class1 Valves Data Sheet Report*. APP-PV03-Z0R-001 Revision 3. Westinghouse Electric Company LLC. TRIM Ref: 2011/473819.
 - 26 *Design Change Proposal APP-GW-GEE-864 Revision 0. SI Accumulator and CMT Outlet Check Valve Design Changes*. Westinghouse Electric Company LLC. September 2009. TRIM Ref: 2011/76327.
 - 27 *Globe Stop Check Valve Stainless Steel*. APP-PV03-V2-013 Revision C. Westinghouse Electric Company LLC. 5 July 2009. TRIM Ref: 2011/479313.
 - 28 *AP1000 Valve Standardization Selection Criteria*. APP-GW-P1-026 Revision 0. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/81425.
 - 29 *AP 1000 Design Specification. 3" and Larger Motor Operated Gate and Globe Valves, ASME Boiler and Pressure Vessel Code Section III class 1, 2, and 3*. APP-PV01-Z0-001 Rev 1. Westinghouse Electric Company LLC – TRIM Ref: 2011/474516.
 - 30 Not used.
-

-
- 31 *Equipment Qualification Methodology and Documentation Requirements for AP1000 Safety-Related Valves and Valve Appurtenances.* APP-GW-VP-010 Revision 2. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/81450.
- 32 *Design Change Proposal APP-GW-GEE-242 Revision 0. Inservice Testing of IRWST Injection Check Valves (V122A, B and V11224A, B) Modification.* Westinghouse Electric Company LLC. TRIM Ref: 2011/209667.
- 33 *WEC00446N Response to Regulatory Observation RO-AP1000-094 and Regulatory Observation Actions RO-AP1000-094.A1-A5, GDA Design Basis Limits and Development of Plant Operating Limits and Maintenance Schedules.* Letter from ND to AP1000 Project Front Office. WEC70285R. 14 January 2011. TRIM Ref: 2011/32025.
- 34 *AP1000 UK Safety Categorisation and Classification Methodology.* UKP-GW-GL-044 Revision 1. Westinghouse Electric Company LLC. 2010. TRIM Ref: 2011/173949.
- 35 *AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components.* UKP-GW-GL-144 Revision 1. Westinghouse Electric Company LLC. January 2011. TRIM Ref: 2011/91066.
- 36 *Design Change Proposal APP-GW-GEE-1258 Revision 0. Addition of Reactor Trip to Mitigate the Inadvertent PRHR Transient.* Westinghouse Electric Company LLC. TRIM Ref: 2011/76305.
- 37 *WEC RO-AP1000-88 Response.* Letter from AP1000 Project Front Office to ND. WEC000317. August 2010. TRIM Ref: 2010/390503.
- 38 *AP1000 Design Specification Diesel Generator Units.* AP-MS40-Z0-001P Revision 2. Westinghouse Electric Company LLC. TRIM Ref: 2011/475379.
- 39 *Review of Nuclear Plant Operating Experience and the Application to the AP600 Design.* WCAP-14115 Revision 0. Westinghouse Electric Company LLC. July 1994. TRIM Ref: 2011/93226.
- 40 *Operating Experience to Apply Advanced Light Water Reactor Designs.* APP-GW-G1R-007 Revision A. Westinghouse Electric Company LLC. March 2006. TRIM Ref: 2011/79456.
- 41 *Operational Assessment for AP1000.* WCAP-15800 Revision 3. Westinghouse Electric Company LLC. July 2004. TRIM Ref: 2011/93259.
- 42 *Project Plan AP1000 Squib Valve.* APP-PV70-VDH-001 Revision 0. Westinghouse Electric Company LLC. December 2008. TRIM Ref: 2011/294097.
- 43 *AP1000 Technical Report Review. Response to Request for Additional Information (RAI).* RAI-SRP6.2.2-CIB1-25 Revision 0. Westinghouse Electric Company LC. TRIM Ref: 2011/209674.
- 44 Not Used.
- 45 *AP1000 Squib Valve Failure Modes and Effects Analysis (FMEA).* APP-PV70-GRA-001 Revision 0. Westinghouse Electric Company LLC. March 2010. TRIM Ref: 2011/94136.
- 46 *Department of Defense Design Criteria Standard, Fuze Design, Safety Criteria for.* MIL-STD-1316E. US Department of Defense. July 1998.
- 47 *Design Change Proposal Squib valve Actuation Time Adjustment.* APP-GW-GEE-908 Rev 0. TRIM Ref: 2011/110971.
- 48 *Service Water System.* Letter from AP1000 Project Front Office to ND. WEC 000485. Westinghouse Electric Company LLC. January 2010. TRIM Ref: 2011/49635.
-

-
- 49 *OM code ISTC 5260 for Operation and Maintenance of Nuclear Power Plants Inservice Testing of Valves in Light–Water Reactor Power Plants.* ASME Standards Technology.
- 50 *Design Change Proposal. ADS Stage 4 Piping Temperature Increase under Plant Normal Operating Conditions.* APP-GW-GEE-1793 Revision 0. Westinghouse Electric Company LLC. August 2010. TRIM Ref: 2011/79488.
- 51 *Design Change Proposal. Change to Squib Valves in PXS IRWST injection lines.* APP-GW-GEE-186 Revision 1. Westinghouse Electric Company LLC. February 1994. TRIM Ref: 2011/81875.
- 52 *Guide for application and use of valves in Power Plant systems.* NP-6516. Electric Power Research Institute (EPRI). August 1990.
- 53 *Valve Standardisation Selection Criteria.* GW-P1-020 Revision 0. Westinghouse Electric Company LLC. 6 March 1996. TRIM Ref: 2011/478084.
- 54 Not used.
- 55 *Design Change Proposal Corrections to PXS P&ID and DCD.* APP-GW-GEE-1297 Revision 0. Westinghouse Electric Company LLC. July 2010. TRIM Ref: 2011/79468.
- 56 *Piping and Instrumentation Diagram, Passive Core Cooling System.* APP-PXS-M6-002 Revision 6. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/94200.
- 57 *Squib Valve Design Specification.* APP-PV70-Z0-001 Revision G. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/94137.
- 58 *Westinghouse 3.3.1 Procedure. Design Reviews.* Westinghouse Electric Company LLC. August 2009. TRIM Ref: 2011/82202.
- 59 Not used.
- 60 *SPX Process Equipment Copes-Vulcan. Design Calculation No. MAC-102210.* TRIM Ref: 2011/478932.
- 61 *Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary.* APP-PV70-GER-002 Revision B. Westinghouse Electric Company LLC. August 2010. TRIM Ref: 2011/94132.
- 62 *Design Report 10.2.189. 8" Class 2500 Squib (Pyrotechnic Actuated) Valve.* APP-PV70-Z0-001 Revision 0. Westinghouse Electric Company LLC. October 2010. TRIM Ref: 2010/571048.
- 63 *Design Report 10.2.190. 8" Class 2500 Squib (Pyrotechnic Actuated) Valve.* APP-PV70-Z0-001 Revision 0. Westinghouse Electric Company LLC. October 2010. TRIM Ref: 2010/571050.
- 64 *Design Report 10.2.191. 14" Class 2500 Squib (Pyrotechnic Actuated) Valve.* APP-PV70-Z0-001 Revision 0. Westinghouse Electric Company LLC. 22 October 2010. TRIM Ref: 2010/564235.
- 65 *Squib Valve Actuator Specification.* APP-PV98-Z0-001 Revision 0. Westinghouse Electric Company LLC. September 2010. TRIM Ref: 2010/523103.
- 66 *Westinghouse Response to RO-AP1000-069, Equipment Qualification.* WEC00487N. Letter from AP1000 Project Front Office to ND. January 2011. TRIM Ref: 2011/57985.
- 67 *UK AP1000 Environment Report.* UKP-GW-GL-790 Revision 3. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/93195.
-

-
- 68 *Squib (Pyrotechnic Actuated) Valves, In-service Test Recommendations.* APP-PV70-VM-001 Revision 0. Westinghouse Electric Company LLC. TRIM Ref: 2010/519119.
- 69 *Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary.* APP-PV70-GER-002 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref: 2011/849.
- 70 *Test Report 10.4.368. Functional Testing Squib (Pyrotechnic Actuated) Valve.* APP-PV70-Z0-001 Revision 0. Westinghouse Electric Company LLC. 25 October 2010. TRIM Refs 2010/571265, 2010/564241, 2010/564252, 2010/564264 and 2010/564295.
- 71 *Nuclear Industry Guidance. An Aid to the Design of Ventilation of Radioactive Areas.* NVF/DG001 Issue 1. January 2009. TRIM Ref: 2011/223574.
- 72 *Overpressure Protection Report for AP1000 Nuclear Power Plant.* WCAP-16779-NP Revision 1. Westinghouse Electric Company LLC. August 2010. TRIM Ref: 2011/93271.
- 73 *Engineering Summary Report for the AP1000 Control rod Drive Mechanism (CRDM) Model L106AP Life Test.* APP-MV11-T2-021 Revision A. Westinghouse Electric Company LLC. January 2010. TRIM Ref: 2011/76370.
- 74 *AP1000 Control Rod Drive Mechanism Failure Mode and Effects Analysis (FMEA).* APP-MV11-GRA-001 Revision 0. Westinghouse Electric Company LLC. October 2008. TRIM Ref: 2011/81481.
- 75 *AP1000 Control Rod Drive Mechanism (CRDM) Latch Assembly Life Test Specification.* APP-MV11-T1-021 Revision 2. Westinghouse Electric Company LLC. September 2009. TRIM Ref: 2011/76367.
- 76 *AP1000 Valve Data Sheet.* APP-PV01-Z0D-131 Revision 2. Westinghouse Electric Company LLC. TRIM Ref: 2011/478913
- 77 *AP1000 LTOPS Analysis/Normal RNS Relief Valve Sizing Evaluation.* APP-RNS-M3C-002 Revision 3. Westinghouse Electric Company LLC. November 2009. TRIM Ref: 2011/81644.
- 78 *Thermal Stratification criteria for AP1000.* APP-GW-P1-005 Revision A. Westinghouse Electric Company LLC. October 2007. TRIM Ref: 2011/81423.
- 79 *8" Squib Valve Arrangement Drawing D-402112* Revision 0. TRIM Ref: 2010/571124.
- 80 Not used.
- 81 *Process and Instrumentation Diagram, Passive Containment Cooling System* APP-PCS-M6-001 and 002. Westinghouse Electric Company LLC. October 2009. TRIM Refs. 2011/76373 (APP-PCS-M6-001) and 2011/76374 (APP-PCS-M6-002).
- 82 *AP1000 In-Plant Design Criteria and Guidelines for the Control of Heavy Loads.* APP-GW-N1-006 Revision 1. Westinghouse Electric Company LLC. February 2009. TRIM Ref: 2011/81418.
- 83 *Continued Reactor Operation with Both Reactor Pressure Vessel Head 'O' Ring Seals Leaking due to Leak-Detection System Design Deficiencies and Lack of Boric Acid Leak Detection Programme.* International Incident Reporting System (IRS) Report Number 7643. Date of Receipt 16/09/2004.
- 84 *Design Change Proposal AP1000 Coastal Site Hardening – VBS & VUS Class 2 Changes.* APP-GW-GEE-767 Revision 1. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/93537.
-

-
- 85 *AP1000 Standard Plant Metrification*. APP-GW-G1-011 Revision 0. Westinghouse Electric Company LLC. November 2009. TRIM Ref: 2011/79448.
- 86 *AP1000 Standard Plant Metrification*. APP-GW-G1-011 Revision 1. Westinghouse Electric Company LLC. April 2010. TRIM Ref: 2011/79450.
- 87 *AP1000 Standard Plant Metrification*. APP-GW-G1-011 Revision 2. Westinghouse Electric Company LLC. September 2010. TRIM Ref: 2011/79451.
- 88 *AP1000 European Design Control Document*. EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC. TRIM Ref: 2011/81804.
- 89 *Qualification Plan for Safety-related Squib Valve Actuators and Electrical Connection Assemblies for Westinghouse Electric Company for use in Westinghouse AP1000 Nuclear Power Plants*. APP-PV70-T5-001 Revision 2. Westinghouse Electric Company LLC. November 2010. TRIM Ref: 2011/100934.
- 90 *Electromagnetic Interference (EMI) Test Procedure for a Squib Valve Initiator and Connection Assembly*. APP-PV70-T5-002 Revision 1. Westinghouse Electric Company LLC. October 2010. TRIM Ref: 2011/100933.
- 91 *Test Report for Production Life Testing of AP-1000 Three Coil Control Rod Drive Mechanism Latch assembly Y/Coil Stack Assemblies*. TR-AP1000 Prototype Revision 00. Westinghouse Electric Company LLC. 2 July 2010. TRIM Ref: 2011/477836.
- 92 *Squib Valve Modelling in the AP1000 PRA*. DCPMIS0254. TRIM Ref: 2011/477828.
- 93 *AP1000 Standard Safety System Termination Unit Assembly Hardware Requirements Specification*. WNA-DS-01496-WAPP Rev 01. Westinghouse Electric Company LLC. April 2009. TRIM Ref: 2010/573999.
- 94 Not used.
- 95 *Engineered Safeguards Actuation System 24-Month Actuation Device Test*. CPP-PMS-GJP-813 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref: 2011/94567.
- 96 *Development Report Pyrotechnic Cartridges for Squib Valves – Westinghouse AP1000 Nuclear Reactor*. 17399 (01)DR. TRIM Ref: 2011/112839.
- 97 *Hohmann C, Tipton W Jr, Dutton M. Propellant for the NASA Standard Initiator*. NASA/TP-2000-210186. NASA Johnson Space Centre, Houston, Texas. October 2000.
- 98 *Hohmann C and Tipton W Jr. Viton's Impact on NASA Standard Initiator Propellant Properties*. NASA/TP-2000-210187. NASA Johnson Space Centre, Houston, Texas. October 2000. <http://ston.jsc.nasa.gov/collections/TRS/techrep/TP-2000-210187.pdf>
- 99 *Single-Failure-Proof Cranes for Nuclear Power Plants*. NUREG-0554. USNRC. May 1979 <http://pbadupws.nrc.gov/docs/ML1104/ML110450636.pdf>
- 100 *A Guide to American Crane Standards. For Electric Overhead Travelling Cranes, Hoists and Related Equipment for Nuclear Facilities. Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. ASME NOG-1. ASME Standards Technology LLC. 2008. ISBN No. 0-7918-3141-8. <http://files.asme.org/catalog/stllc/printbook/20530.pdf>.
- 101 *A Survey of Crane Operating Experience at US Nuclear Power Plants from 1968 through 2002*. NUREG 1774. USNRC. <http://pbadupws.nrc.gov/docs/ML0320/ML032060160.pdf>.
- 102 *OM Code for Operation and Maintenance of Nuclear Power plants*. ASME Standards Technology LLC. 2009. ISBN: 9780791832271.
-

- 103 *Fuzing Systems – Safety Design Requirements*. NATO STANAG 4187. NATO. 9 March 2007.
- 104 *GDA Issue GI-AP1000-ME-01 Revision 1. Background and explanatory information*. TRIM Ref: 2011/81334.
- 105 *GDA Issue GI-AP1000-ME-02 Revision 1. Background and explanatory information*. TRIM Ref: 2011/81321.
- 106 *GDA Issue GI-AP1000-ME-03 Revision 0. Background and explanatory information*. TRIM Ref: 2011/102493.
- 107 *Step 4 Cross-cutting Topics Assessment of the Westinghouse AP1000[®] Reactor*. ONR Assessment Report ONR-GDA-AR-11-016 Revision 0. TRIM Ref: 2010/581515.

Table 1

Relevant Safety Assessment Principles for Mechanical Engineering Considered During Step 4

SAP No.	SAP Title	Description
FP series	Fundamental principles	FP.1 to FP.8
SC series	Safety cases	SC.1 to SC.8
EKP series	Key principles	EKP.1 to EKP.5
ECS series	Safety classification and standards	ECS.1 to ECS.5
EQU series	Equipment qualification	EQU.1
EDR series	Design for reliability	EDR.1 to EDR.4
EMT series	Maintenance, inspection and testing	EMT.1 to EMT.8
EAD series	Aging and degradation	EAD.1 to EAD.5
ELO series	Layout	ELO.1 to ELO.4
EHA series	External and internal hazards	EHA.1 to EHA.17
EPS series	Pressure systems	EPS.1 to EPS.5
ESS series	Safety systems	ESS.1 to ESS.27
EES series	Essential services	EES.1 to EES.9
ECV series	Containment and ventilation	ECV.1 to ECV.10
EHT series	Heat transport systems	EHT.1 to EHT.5
AM series	Accident management and emergency preparedness	AM.1

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-01	The licensee shall generate appropriate evidence that Equipment Qualification is adequately specified for all mechanical items important to safety	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-02	The licensee shall make available upon request evidence of the detailed design substantiation, FATs information, and SATs information, for individual mechanical items and their associated systems, which are important to safety.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-03	The licensee shall ensure that design changes associated with the AP1000, specifically including Class 3 DCPs, are adequately controlled, and receive a suitable degree of review and audit, commensurate with their safety significance.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-04	The licensee shall ensure that the final manufactured items important to safety meet the safety important requirements set forth in the final design documentation.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1**Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business****Mechanical Engineering – AP1000**

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-05	The licensee shall ensure that the appropriate safety function categorisation and equipment classification methodology is cascaded through all necessary design and safety documentation to support the AP1000 NPP design. This exercise should specifically include equipment which is the source of postulating initiating events (i.e. safety related systems, also termed duty systems).	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-06	The licensee shall review and consider alternative materials to Stellite™ for applications within the NPP domain, and ensures that the final selection of materials for the AP1000 is ALARP in this respect.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-07	The licensee shall provide evidence that they have adequately accounted for the 'dead leg' phenomenon in the pipework design of the AP1000.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-08	The licensee shall generate the design principles, philosophy, and ALARP arguments to manage the risk of inappropriate tampering of manually operated valves throughout the AP1000 design; whilst ensuring that valves can be operated on demand without unnecessary complication.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-09	The licensee shall ensure that evidence is generated to ensure that the proposed codes and standards for the AP1000 are adequate to support design, procurement, installation, operation, and subsequent EMIT activities. The licensee should also ensure that the AP1000 codes and standards meet applicable UK Health and Safety legislation, including regulations and ACOPs (as appropriate).	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-10	The licensee shall make and implement adequate arrangements to ensure the AP1000 NPP design for the UK recognises as necessary changes to applicable codes, standards, and legislation.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-11	I consider it to be an Assessment Finding that a future licensee shall carry out an inspection of the shims during the NPP operational life. In clarification, my expectation is that visual inspection of a CRDM shim should be carried out following the replacement of a latch assembly, without the need for a routine scheduled maintenance inspection requirement.	During operational phase as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-12	The licensee shall ensure that the design change associated with spurious operation of the PRHR HX has been completed to ensure that the reactor is tripped as necessary, and that all necessary AP1000 design and safety documentation has been updated accordingly.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-13	The core make-up discharge lines in-line check valves are to be tested during each planned outage for disk closure, disk passing, and reopening on no flow. Testing is achieved via the system design incorporating a dedicated pipework arrangement, which forms part of the primary reactor coolant circuit and is isolated appropriately via an isolation valve and welded plug. This arrangement is being introduced into the design via a design change, which is currently progressing through the Westinghouse due process. The licensee shall ensure that this design change has been completed, and all necessary AP1000 design and safety documentation has been updated accordingly.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-14	The licensee shall generate an ALARP argument to justify each application of stop check valve within the AP1000 NPP design.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-15	The sizing evaluation for the LTOPS contains four open items, since some of the parameters used in the calculation were not finalised at the time of production of the report. The licensee shall ensure that the LTOPS justification has been completed and all open items have been satisfactorily closed out.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-16	The licensee shall generate evidence that the Reactor Coolant Pump seals have adequately considered the effect of radiation ageing for a 60 year design life.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-17	The licensee shall generate the formal approved copy of the applicable Reactor Coolant Pump Design Specification for possible confirmatory assessment as normal regulatory business.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-18	The licensee shall develop an adequate EMIT strategy for the AP1000 Reactor Coolant Pumps, with due consideration to the manufacturer's recommendations for preventative maintenance.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-19	The licensee shall generate evidence that the AP1000 proposed pump design can be installed and replaced with adequate consideration to UK legislation requirements and without having a negative impact on adjacent SSCs that are considered important to safety. This should also include justification for the use of temporary equipment (e.g. steel plates) during this process, as opposed to permanent features.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-20	The licensee shall ensure that an appropriate safety classification is assigned to the RCP flywheel.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-21	The licensee shall generate an adequate strategy for verifying the safety functional requirement of RCP flywheel coast-down performance during the operational lifetime of the NPP.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business
Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-22	The licensee shall ensure that the AP1000 load path determination activity is completed, and this load path determination should take into account ALARP principles. In particular Westinghouse has identified that a heavy lift involving the Cask Handling Crane is undertaken in a room above the Normal Residual Heat Removal Heat Exchangers, and the design presently relies on administrative control only to ensure that the load path / route is clear of the area directly above these heat exchangers. I consider this to be an example of where physical barriers could be provided to prevent inadvertent handling of this heavy load over this sensitive area, and the practicability of provision of barriers should be reviewed on the basis of ALARP principles.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-23	The licensee shall ensure that all lifts of nuclear safety significance are identified, and safe load paths are specified through appropriate design and safety documentation, and procedures.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-24	The licensee shall ensure that the design of rigging equipment associated with lifts of nuclear safety significance has been completed, and these designs have been assessed to minimise the possibility of human error based on ALARP principles.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-25	The licensee shall ensure that the design changes associated with the provision of passive HEPA filtration for the nuclear ventilation systems in response to RO-AP1000-043 have been completed and that all necessary AP1000 design and safety documentation has been updated accordingly.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-26	The licensee shall ensure that an adequate design substantiation has been generated for the ventilation design changes, specifically 'blow out panels', made in response to the Regulatory Observation regarding the Spent Fuel Pool DBA requirement (RO-AP1000-054, Ref. 11).	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-27	The licensee shall establish an appropriate filter change doctrine for all safety important filters within the nuclear ventilation systems.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-28	The licensee shall ensure that design changes (APP-GW-GEE-767) associated with the 'hardening' of the nuclear ventilation external features to accommodate the UK maritime climate / weather have been completed and that all necessary AP1000 design and safety documentation has been updated accordingly.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-29	Westinghouse has stated that further changes considered necessary to harden the ventilation systems will be described as expected changes for coastal sites in the update of the PCSR due at the end of the GDA process. The licensee shall ensure that these changes are implemented for the AP1000 design for UK coastal site applications.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

**Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business
Mechanical Engineering – AP1000**

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-30	The licensee shall verify the site specific design air temperatures and humidity values against those used as the basis for the AP1000 design, to ensure that the nuclear ventilation systems can adequately perform their safety functions.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - delivery to site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-31	The licensee shall ensure that the design change associated with the increase in nuclear ventilation stack height has been completed and that all necessary AP1000 design and safety documentation has been updated accordingly.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-32	The licensee shall ensure that any fume cupboards within the AP1000 are not used for the containment of radioactive substances.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-33	The licensee shall ensure that the RNS / SFP heat transfer calculations are reviewed against the site specific predicted temperatures / conditions, to ensure that the design remains adequate.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-34	The licensee shall assess the practicability of inspecting and / or replacing detrimentally affected sections of the CCS in respect of corrosion, and implement any necessary ALARP improvements which are identified.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-35	I am aware that the original design or the AP1000 used a common discharge and suction header for both trains of the SFS. A design change was then instigated to provide separate discharge and suction headers to the spent fuel pool. The licensee shall ensure that this design change is fully reflected in all necessary design and safety documentation.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-36	The licensee shall generate evidence that the diesel generator systems that have now been assigned as being important to safety have adequately considered Operational Experience Feedback in terms of their design and EMIT requirements.	Install diesel generators complete as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-37	Westinghouse's response to TQ-AP1000-1002 (Ref.10) failed to answer the question posed on the amendment to the Motor Fuel (Composition and Content) Regulations 1999, which is to be implemented under EU Directive 2009/30/EC. The licensee shall generate arguments and evidence to ensure the proposed diesel generator designs consider and comply with the revised fuel regulations.	Install diesel generators complete as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-38	Westinghouse stated that they are now confident that following the IRWST design modification, the screen design and associated system would be acceptable to the US NRC. The licensee shall ensure that this design change, incorporating adequate consideration of any further comments from the US NRC, has been incorporated into the AP1000 design and they report the satisfactory outcome of the test programme.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-39	The licensee shall ensure that the seals for the Equipment Hatch and Personnel Airlock are changed at every outage, or an alternative EMIT strategy justified, and this is reflected in the EMIT documentation.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Mechanical Engineering – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-ME-40	The licensee shall ensure that the design of the RPV leak detection system is reviewed against the findings of the IRS 7643 report, improvements identified as necessary, and justification provided as to why the design system is considered to be ALARP.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-41	The licensee shall review the safety case Operational Limits and Conditions to ensure that procedures are adequate to detect any passing of the outer RPV seal, such as measurements of containment activity, humidity, and drainage.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-42	The licensee shall develop adequate EMIT procedures for the detection of leaks of boric acid generally within containment.	Fuel on-site as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.
AF-AP1000-ME-43	The licensee shall ensure that the containment safety system to protect against the partial vacuum phenomenon has been fully incorporated into the AP1000 design and safety documentation.	Mechanical, Electrical and C&I Safety Systems, Structures and Components - inactive commissioning as this is the appropriate point when sufficient evidence should be available to demonstrate this requirement for Mechanical Engineering.

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

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Mechanical Engineering – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION

GI-AP1000-ME-01 REVISION 1

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A1
GDA Issue	<p>While undertaking the GDA the availability of adequate arguments and evidence for the selection, system incorporation and qualification of the squib valve designs has been limited.</p> <p>Westinghouse is required to issue appropriate approved documentation that provides adequate arguments and evidence for their selection, equipment design, and associated system design.</p>		
GDA Issue Action	<p>Generate and issue appropriate approved documentation that provides adequate arguments and evidence for the squib valve selection.</p> <p>ONR considers a GDA can not be completed without the design being finalised and the availability of auditable and approved design documentation that demonstrates the valve selection at the concept stage is ALARP.</p> <p>ONR's expectation is for Westinghouse to finalise their designs and provide the formal Summary Report, which is to include the appropriate arguments and evidence to demonstrate the squib valve selection is ALARP, with sufficient evidence of optioneering, and the design has followed a robust design process.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

**WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1**

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A2
GDA Issue Action	<p>Generate and issue appropriate approved documentation to justify the squib valve detailed component designs are able to achieve the safety case requirements and assumptions.</p> <p>ONR considers a GDA can not be completed, without the designs being finalised and the availability of approved design documentation that demonstrates the valve detailed component designs meets the safety case requirements.</p> <p>ONR’s expectation is for Westinghouse to finalise their designs and provide the formal approved design justification, which includes the appropriate arguments and evidence that the valves’ detailed component designs meet the safety functional requirements.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A3
GDA Issue Action	<p>Generate and issue appropriate approved documentation to justify that the squib valve interfacing system designs (e.g. supports, interfacing pipework etc.) are able to achieve the safety case requirements and assumptions.</p> <p>ONR considers a GDA can not be completed, without the designs being finalised and the availability of approved design documentation that demonstrates each valve is integrated into its associated system, and meets the safety case requirements.</p> <p>ONR's expectation is for Westinghouse to finalise their designs and provide the formal approved design justification, which includes the appropriate arguments and evidence that each valve is integrated into its associated system, and meets the safety functional requirements.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

**WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1**

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A4
GDA Issue Action	<p>Generate and issue appropriate approved documentation to demonstrate the surveillance and EMIT regime is able to achieve the safety case requirements and assumptions. Given the 60 year design life of the AP1000, and the inability to stroke the squib valves during in service inspections, ONR considers that Westinghouse needs to specify a robust surveillance regime to ensure that the squib valve designs are capable of delivering their safety functions in accordance with the requirements of the safety case.</p> <p>ONR’s expectation is for Westinghouse to finalise their designs and provide the formal approved design justification, which is to include an adequate surveillance and EMIT regime specification that is commensurate to the AP1000 NPP safety case and the safety role for each squib valve type.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A5
GDA Issue Action	<p>Westinghouse shall address the listed points, which have been identified as gaps in the safety justification of the squib valve designs as a result of undertaking the GDA from a Mechanical Engineering perspective:</p> <ul style="list-style-type: none"> • Westinghouse shall demonstrate the FMEA for the final squib valve designs includes an independent technical reviewer. • Westinghouse shall generate and issue an ALARP justification that each squib valve type as proposed is adequate to achieve its safety functional requirements and its design intent, in terms of position indication during normal operation. • Westinghouse shall generate and issue an ALARP statement on how the bracket design achieves the design intent of a guard. • Westinghouse shall generate and issue an ALARP statement on how the 14 inch ADS squib valve design achieves its design intent without the requirement of a cover. • Westinghouse shall provide confirmatory evidence of the described poka yoke features within the 8 inch valve detailed drawings. • Westinghouse shall provide evidence that adequate arrangements are in place to control and manage the supply of the squib valves, and tolerances for the technical parameters of critical components. • Westinghouse shall provide evidence that the squib valve Equipment Qualification tests adequately demonstrate that each squib valve type is able to achieve its design intent. <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

**WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1**

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A6
GDA Issue Action	<p>Westinghouse shall address the listed points, which have been identified as gaps in the safety justification of the squib valve designs as a result of undertaking the GDA from a Pyrotechnics perspective:</p> <ul style="list-style-type: none"> • Westinghouse shall issue document (#35 (APP-PV70-GER-001)). • Westinghouse shall generate and issue the arguments and evidence regarding the following items: <ul style="list-style-type: none"> - Justify why different rationales have been adopted to select the pyrotechnic substances for the initiator and booster. - Demonstrate why good practice from aerospace is relevant within nuclear plants. - Justify the choice regarding the binder; notably, a comprehensive and well-argued analysis and supporting evidence requires to be provided. - Provide results of radiation exposure of the propellants, and the demonstration that reference environments used in the past are sufficiently similar to the environment expected within AP1000 reactors. - The relevance of the Summary Report, Appendix C in substantiating the pyrotechnics aspects. • Westinghouse shall generate an argument that demonstrates that: <ul style="list-style-type: none"> - Test data from carrying out initiator tests by others provides suitable reliability evidence for use with the AP1000 design given the variance in the AP1000 initiator design and the use of a binder. - Sufficient and relevant test evidence exists for the AP1000 booster design to support its reliability claim. • Westinghouse shall clarify the relevance and purpose of Development Report 17399(01)DR to the ballistic analysis. • Westinghouse shall provide: <ul style="list-style-type: none"> - A review of the advantages and disadvantages of each considered initiator concept. - An explanation of the selection criterion for the initiator ignition concept. - The analysis to support the selection of each considered initiator concept. • Westinghouse shall generate and issue the justification that: <ul style="list-style-type: none"> - Cartridges will not be liable to react to any electromagnetic environments, with adequate consideration to resonant harmonics that they will be exposed to throughout their life cycle. 		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION

GI-AP1000-ME-01 REVISION 1

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A6
	<ul style="list-style-type: none"> - EMIT requirements for EMI protection is suitable and adequate. • Westinghouse shall generate and issue the justification that all the relevant UK requirements for the design of cartridges and termination units have been adequately covered by the implementation of US standards and guidance. • Westinghouse shall generate and issue the following documentation: <ul style="list-style-type: none"> - Finalised requirements regarding the propellant neutron testing, by justifying the energy, the intensity, and the duration of exposure. - Qualification results, which includes the substantiation that actuators as proposed are adequate to achieve their safety functional requirements and their design intent. • Westinghouse shall provide the justification that C&I faults do not impact the properties of the initiator bridgewire. • Westinghouse shall generate and issue a further analysis to confirm that, in case of a fire in adjacent containment fire zones, the present design of cartridge peak temperature is maintained below the propellant auto-ignition temperature with an adequate margin. To date fires in surrounding rooms have not adequately considered. • Westinghouse shall generate and issue comprehensive justification that: <ul style="list-style-type: none"> - The safeguards that are provided within the termination units and cabinet interface modules are sufficient to reduce the spurious actuation probability at a level coherent with other potential sources of LOCA. - The absence of SADs within the pyrotechnic chain achieves the correct balance between the two competing demands of preventing spurious actuation of the squib valves, and yet ensuring they have a high reliability of actuation on demand to support the passive core cooling function. • In respect of the electrical current values Westinghouse shall provide: <ul style="list-style-type: none"> - A review of the advantages and disadvantages of each considered value. - An explanation of the selection criterion for the electrical current value. - The analysis to support the selection of each considered option. • Westinghouse shall generate and issue the justification that each squib valve termination unit type and terminal block is designed adequately to achieve its safety functional requirements and its design intent. This justification shall include: <ul style="list-style-type: none"> - The comprehensive list of safety and functional requirements, including surveillance monitoring requirements. - The detailed description of design solutions. 		

Annex 2**WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT****GDA ISSUE****SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION****GI-AP1000-ME-01 REVISION 1**

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A6
	<ul style="list-style-type: none"> - The qualification programme and its results. - The description of EMIT provisions required to maintain safety functions. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SQUIB VALVE CONCEPT AND DESIGN SUBSTANTIATION
GI-AP1000-ME-01 REVISION 1

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		Probabilistic Safety Assessment Fault Studies	
GDA Issue Reference	GI-AP1000-ME-01	GDA Issue Action Reference	GI-AP1000-ME-01.A7
GDA Issue Action	<p>Westinghouse shall address the listed points, which have been identified as gaps in the safety justification of the squib valve designs as a result of undertaking the GDA from a Surveillance and EMIT perspective:</p> <ul style="list-style-type: none"> • Westinghouse shall provide the detailed evidence that an adequate visual inspection can be carried out on the 8 inch squib valve design. • Westinghouse shall explicitly capture in the consolidated PCSR the requirement that if a cartridge taken out of a plant fails its test then all cartridges from that batch should be replaced. • Westinghouse shall generate and issue the justification that electrical testing EMIT requirements result from a process which has considered and analysed each option, with a suitable selection rationale. This justification shall demonstrate specifically the following items: <ul style="list-style-type: none"> - Testing every 24 months is sufficient to prove a high level of availability of the safety system using squib valves. - Insulation testing does not reduce the risk of failure. - Electrical currents supplied by digital voltmeters always stay lower than the threshold defined in bridgewire resistance test. - Reconnecting initiators to a circuit under voltage does not increase the risk. • Westinghouse shall identify in the safety case that every cartridge subjected to a significant mechanical shock loading during its lifetime must not be used, as a safety requirement. As part of this, Westinghouse shall also define the acceptance parameters in respect of this criterion. • Westinghouse shall generate evidence of recommending an adequate surveillance and EMIT regime that is commensurate to the AP1000 NPP safety case assumptions and the safety role of each squib valve type. <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT**GDA ISSUE****METRICATION OF MECHANICAL EQUIPMENT AND CIVIL STRUCTURAL STEELWORK CONNECTIONS****GI-AP1000-ME-02 REVISION 1**

Technical Area		MECHANICAL ENGINEERING AND CIVIL ENGINEERING	
Related Technical Areas		Cross-cutting	
GDA Issue Reference	GI-AP1000-ME-02	GDA Issue Action Reference	GI-AP1000-ME-02.A1
GDA Issue	<p>The Guidance to Requesting Parties requires that documents submitted for GDA use SI units. As a corollary it is the expectation that the design submitted by the Requesting Party is essentially metric, using metric Structures, Systems and Components. ONR has provided advice to clarify the detail of its expectations, and to allow variation from this expectation for a limited, controlled, and justified sub-set of equipment.</p> <p>ONR does not consider that Westinghouse has satisfactorily met this expectation for mechanical equipment and associated systems. This issue also affects civil structural steelwork.</p>		
GDA Issue Action	<p>Provide an updated response to document titled 'AP1000 Standard Plant Metrication, APP-GW-G1-011', to reflect the guidance provided by ONR. Westinghouse should commit to re-designing equipment in line with the guidance, or provide a more rigorous justification (which aligns with the guidance provided) as to why they consider equipment should be an exception to metrication.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT**GDA ISSUE****METRICATION OF MECHANICAL EQUIPMENT AND CIVIL STRUCTURAL STEELWORK CONNECTIONS****GI-AP1000-ME-02 REVISION 1**

Technical Area		MECHANICAL ENGINEERING AND CIVIL ENGINEERING	
Related Technical Areas		Cross-cutting	
GDA Issue Reference	GI-AP1000-ME-02	GDA Issue Action Reference	GI-AP1000-ME-02.A2
GDA Issue Action	<p>Provide an updated response to document titled 'AP1000 Standard Plant Metrication, APP-GW-G1-011 Rev 3' to explicitly list the exclusions from metrication for Civil Steelwork SSCs. This should include Westinghouse's intention for all the component parts of structural steelwork connections. It is accepted that the generic design for permanent civil steel structures is based on imperial sections (and materials). However, the exceptions listed in Table A-1 of APP-GW-G1-011 Rev 3 do not clearly define what approach will be used for the design of the detailed connections which will be carried out by local suppliers.</p> <p>The widescale used of imperial bolting / fastenings is not acceptable. Although strict quality control during construction can be adopted, there is an increased risk of last minute substitutions with locally supplied, metric bolts. APP-GW-G1-011 Rev 3 does not confirm whether the supplier's design will be quasi metric and or in imperial. The update of this document should clarify Westinghouse's intentions on this, and discuss the effects if the other approach is used.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

**WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
MECHANICAL SYSTEM PIPEWORK DESIGN
GI-AP1000-ME-03 REVISION 0**

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		None	
GDA Issue Reference	GI-AP1000-ME-03	GDA Issue Action Reference	GI-AP1000-ME-03.A1
GDA Issue	<p>Westinghouse is required to provide further justification for the pipework design of the AP1000 for systems important to safety. In particular Westinghouse is required to justify that the AP1000 system designs incorporate adequate isolation and drainage arrangements to enable all anticipated EMIT activities to be carried out in a safe and controlled manner.</p>		
GDA Issue Action	<p>Westinghouse shall generate the arguments and evidence to justify that each isolation that proposes to use pipe freezing technology is ALARP.</p> <p>Westinghouse’s proposal to use pipe freezing technology to provide process isolation in support of their planned EMIT regime is considered not to be good engineering practice for the anticipated isolation requirements for a new reactor design, but rather a technology utilised to recover from a scenario that has not been generally predicted.</p> <p>ONR considers that good engineering practice for a new modern NPP incorporates adequate engineered arrangements for anticipated and planned process isolation to support EMIT activities.</p> <p>ONR’s expectation is for Westinghouse to review their design and either revise their proposal in line with ONR expectations or demonstrate with appropriate arguments and evidence that the anticipated process isolations that propose the use of pipe freezing technology are ALARP.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
MECHANICAL SYSTEM PIPEWORK DESIGN
GI-AP1000-ME-03 REVISION 0

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		None	
GDA Issue Reference	GI-AP1000-ME-03	GDA Issue Action Reference	GI-AP1000-ME-03.A2
GDA Issue Action	<p>Westinghouse shall generate the arguments and evidence to justify that EMIT isolations that rely on single valve isolations are ALARP.</p> <p>The IRWST isolation is provided by a single isolation valve to undertake EMIT of the injection squib valves. This does not achieve ONR expectations when considering the IRWST has a capacity circa 2100m³ and if the single isolation valve was to fail (in its isolation function) then a significant hazard would arise. The system design does not have any other provision to contain the fluid within the IRWST.</p> <p>ONR considers a system isolation first design choice is provided by a suitable valve arrangement, with double valve isolation being provided for systems that are subject to a significant pressure, or temperature, or where there is some other significant hazard e.g. a large volume of fluid is held back.</p> <p>ONR's expectation is for Westinghouse to review their design and either revise their proposal in line with ONR expectations or demonstrate with appropriate arguments and evidence that all anticipated isolations that propose to use single isolation that are the subject of either a significant pressure, temperature or some other significant hazard are ALARP.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
MECHANICAL SYSTEM PIPEWORK DESIGN
GI-AP1000-ME-03 REVISION 0

Technical Area		MECHANICAL ENGINEERING	
Related Technical Areas		None	
GDA Issue Reference	GI-AP1000-ME-03	GDA Issue Action Reference	GI-AP1000-ME-03.A3
GDA Issue Action	<p>Westinghouse shall generate the arguments and evidence to justify that all process pipework designs are adequately engineered to provide drainage facilities to enable the anticipated EMIT activities to be carried out in a safe and controlled manner.</p> <p>Isolation of the motor operator valve to allow EMIT to be carried out on the 4th Stage Squib valves requires the downstream leg of fluid to be drained by ad hoc means i.e. splitting of flanges and use of temporary fluid collection containers. This is an example of the AP1000 design not incorporating adequate engineered arrangements for carrying out anticipated EMIT in a safe and controlled manner.</p> <p>ONR considers that a system design should incorporate adequate engineered arrangements to enable the process pipework to be drained in a safe and controlled manner.</p> <p>ONR's expectation is for Westinghouse to review their design and either revise their proposal in line with ONR expectations or demonstrate with appropriate arguments and evidence that the AP1000 design incorporates adequate engineered drainage facilities to enable anticipated EMIT activities to be carried out in a safe and controlled manner.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>		

Further explanatory / background information on the GDA Issues for this topic area can be found at:	
GI-AP1000-ME-01 Revision 1	Ref. 104.
GI-AP1000-ME-02 Revision 1	Ref. 105.
GI-AP1000-ME-03 Revision 0	Ref. 106.