Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Internal Hazards Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-001
Revision 0
11 November 2011

COPYRIGHT

First published December 2011

PREFACE

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

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

EXECUTIVE SUMMARY

This report presents the findings of the Internal Hazards Assessment of the Westinghouse 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 2 the claims made by Westinghouse were examined, in Step 3 the arguments that underpin those claims were examined.

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 the claims and arguments made in the safety documentation, building on the assessments already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the internal hazards 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 internal hazards an assessment plan for Step 4 was set-out in advance.

My GDA Step 4 assessment was based on the findings from the Step 3 assessment, my assessment of the 2009 Pre-construction Safety Report, the European Design Control Document and Westinghouse's responses to Technical Queries and Regulatory Observations contained in the Master Submission List and inspecting the evidence supporting the design development. The 2009 Pre-construction Safety Report was found to have significant shortfalls in terms of content and quality. Recognising the shortfalls with the 2009 Pre-construction Safety Report, Westinghouse submitted a replacement draft Pre-construction Safety Report in December 2010, which extensively restructured and enhanced the 2009 Pre-construction Safety Report in order to address Nuclear Directorate's concerns. Westinghouse then submitted an approved Pre-construction Safety Report in March 2011 but this was too late for a meaningful assessment during Step 4. Notwithstanding the GDA Issues raised within my assessment, I have no fundamental reasons to believe that Westinghouse cannot produce an adequate Pre-construction Safety Report to support their GDA application, based on the information I have assessed.

My assessment has focussed on the adequacy of hazard identification and prevention as well as on the aspects of redundancy, segregation, and separation that are included within the design to provide mitigation in the unlikely event that such internal hazards should occur. My assessment included:

- Internal hazards in the areas of internal fire, internal flooding, pressure part failure, internal explosion internal missile, and dropped loads and impact.
- Undertaking deep slice sampling of the evidence for a number of areas, including, common cause failure, part pressure failure, internal explosion and internal missile generation.

There have been no items identified as being outside the scope of the GDA process.

From my assessment, I have concluded that:

- There are areas where the safety case presented for internal hazards fails to adequately address the requisite claims, arguments, and evidence which has resulted in the generation of 6 GDA Issues comprising of a total of 9 GDA Issue Actions. Notwithstanding the GDA Issues raised within my assessment, I believe that the AP1000 layout in respect to internal hazards is clear and logical, and one which has been developed through appropriate consideration of

standards, guidance, and relevant good practice. The approach followed within the PCSR for the structure and presentation of the internal hazards safety case may be the basis of the shortfalls identified as in a number of cases there is detailed supporting information presented within the references. As a result, the GDA Issues should be relatively straightforward to address and incorporate in the revised PCSR.

- Throughout Step 4 Westinghouse have adopted a reactive approach to addressing the shortfalls. This led to documentation being produced in response to assessment concerns, and this documentation being supplied in parallel with the assessment. This may also explain some of the inconsistency I have identified within the PCSR documentation of the internal hazards safety case.
- The quality of the information provided coupled with the technical exchanges that have taken place during Step 4 has improved significantly from Step 3. Westinghouse has a far clearer understanding of the UK regulatory regime as well as of the approach taken to safety case production for internal hazards. It should be recognised that the approach taken within the US does not include consideration of internal hazards as a discrete part of the safety case. The approach taken is to assess the hazards as part of the work done within individual engineering disciplines, therefore, drawing all the information together in a coherent manner has proved to be a significant undertaking.
- In all areas of my assessment where GDA Issues have been identified, Westinghouse has understood my concerns and believes that they are largely attributable to the differing regulatory approaches between the US and the UK. I expect Westinghouse to provide more detailed analysis in support of the PCSR for GDA and Westinghouse has accepted that GDA Issues are the most appropriate mechanism to address the safety case shortfalls identified as a result of my Internal Hazards Assessment.

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:

- Substantiation of the barriers in place to prevent fire spread affecting more than one train or division and the need to substantiate fire damper provision.
- Provision of a revised safety case for internal flooding as Westinghouse has now identified shortfalls in the claims, arguments and evidence included within the PCSR issued previously.
- Identification and substantiation of all nuclear significant pipe whip restraints, barriers and shields claimed for the protection of redundant trains against the effects of pressure part failure.
- Provision of substantiation to support claims and arguments made within the area of internal explosion, specifically associated with hydrogen generation within battery rooms and the distribution of hydrogen within areas containing Class 1 Structures, Systems and Components (SSC).
- Identification and substantiation of the claims, arguments and evidence that constitute the internal missile aspects of the internal hazards safety case.
- Substantiation including supporting analyses of the consequences of dropped loads and impact from lifting equipment included within the AP1000 design.

As can be expected there are some areas where there has been a lack of detailed information which has limited the extent of my assessment. This is detailed information relating to the evidence provided which would not have been expected to be submitted as part of the GDA. As a

result HSE will need additional information in the longer term to underpin my conclusions. I have identified this information as Assessment Findings that will be carried forward as part of normal regulatory business. My assessment findings are listed in Annex 1 and typical example is to provide detailed supporting analysis associated with evidence associated with fire barrier penetrations, management procedures associated with cable tray filling, passive cable tray protection, and categorisation and classification.

In my opinion, based upon the information provided in the PCSR and supporting documentation submitted as part of the GDA process, there are no fundamental reasons for believing that a satisfactory safety case cannot be made for the generic AP1000 reactor design, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward work programme for this reactor. It must also be recognised that some of these GDA Issues may ultimately require changes to the plant design. It is therefore too early to rule out the need for changes to plant layout or the provision of additional safety systems.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
ASME	American Society of Mechanical Engineers
BEZ	Break Exclusion Zone
BMS	(ND) Business Management System
BS	British Standards
CA	SC Module – not forming part of the shield building cylindrical wall
CCS	Component Cooling Water System
C&I	Control and Instrumentation
CIV	Containment Isolation Valve
CMT	Core Make-up Tank
COMAH	Control of Major Accident Hazards
COSHH	Control of Substances Hazardous to Health
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DBA	Design Basis Accident
DC	Direct Current
DG	Diesel Generator
EDCD	European Design Control Document
EMI	Electromagnetic Interference (EMI)
FPS	Fire Protection System
GDA	Generic Design Assessment
HBM	Hazard Barrier Matrix
HSE	Health and Safety Executive
HVAC	Heating Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IDS	Standby Electrical Supply System
IEEE	Institute of Electrical and Electronic Engineers
IRWST	In-Containment Refuelling Water Storage Tank
LBB	Leak Before Break
LFL	Lower Flammability Limit
LOCA	Loss of Coolant Accident
LOOP	Loss Of Offsite Power
LPS	Loss Prevention Standards
MCR	Main Control Room
MSIV	Main Steam Isolation Valve

LIST OF ABBREVIATIONS

ND	Nuclear Directorate
NI	Nuclear Island
ONR	Office of Nuclear Regulation
PCCWST	Passive Containment Cooling Water Storage Tank
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PGS	Plant Gas System
P&ID	Process and Instrumentation Diagrams
PIE	Potential Initiating Event
PPF	Part Pressure Failure
PRA	Probabilistic Risk Analysis
PRHA	Pipe Rupture Hazard Analysis
PRHR	Passive Residual Heat Removal
PWS	Potable Water System
PXS	Passive Core Cooling System
RCA	Radiologically Controlled Area
RCDT	Reactor Coolant Drain Tank
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
ROA	Regulatory Observation Action
RSR	Remote Shutdown Room
SAPs	HSE Safety Assessment Principles
SFS	Spent Fuel Cooling System
SG	Steam Generator
SGS	Steam Generator System
SSC	Structure, System and Component
SSD	System Specification Documents
SWS	Service Water System
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
TQ	Technical Query
US NRC	United States Nuclear Regulatory Commission
VBS	Nuclear Island Non-Radioactive Ventilation System
VES	Main Control Room Emergency Habitability System
WEC	Westinghouse Electric Company LLC

LIST OF ABBREVIATIONS

WENRA	Western European Nuclear Regulators' Association
ZOI	Zone of Influence

TABLE OF CONTENTS

Tables

Annexes

Figures

1 INTRODUCTION

1 This report presents the findings of the Step 4 Internal Hazards Assessment of the AP1000 reactor Pre-construction Safety Report (PCSR) (Ref. 1) and supporting documentation provided by Westinghouse under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the PCSR and the supporting evidentiary information derived from the Master Submission List (Ref. 2). The approach taken was to assess the principal submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of the Nuclear Directorate's (ND) Business Management System (BMS) procedure AST/001 (Ref. 3). The Safety Assessment Principles (SAPs) (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 My GDA Step 4 assessment was based on the findings from the Step 3 assessment (Ref. 17), my assessment of the 2009 Pre-construction Safety Report (Ref. 6), the European Design Control Document (Ref. 19) and Westinghouse's responses to Technical Queries and Regulatory Observations contained in the Master Submission List and inspecting the evidence supporting the design development. The 2009 Pre-construction Safety Report was found to have significant shortfalls in terms of content and quality. Recognising the shortfalls with the 2009 Pre-construction Safety Report, Westinghouse submitted a replacement draft Pre-construction Safety Report in December 2010 (Ref. 1), which extensively restructured and enhanced the 2009 Pre-construction Safety Report in order to address Nuclear Directorate's concerns. Westinghouse then submitted an approved Pre-construction Safety Report in March 2011 but this was too late for a meaningful assessment during Step 4.

3 During the assessment a number of Technical Queries (TQ) and one Regulatory Observation (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.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR INTERNAL HAZARDS

4 The intended assessment strategy for Step 4 for the internal hazards topic area was set out in an assessment plan that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below:

2.1 Assessment Plan

5 The Step 4 Internal Hazards Assessment Plan for AP1000 (Ref. 5) identified that the objective of the Step 4 assessment was to review the safety aspects of the proposed reactor designs by examining the evidence, supporting the claims and arguments made in the safety documentation, building on the assessments already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the internal hazards information contained within the PCSR and supporting documentation.

6 The overall bases for the start of assessment in GDA Step 4 were the internal hazards elements of:

- The update to the Submission/PCSR/Supporting Documentation and the Design Reference that relates to the Submission/PCSR. These submissions should fulfil the requirements of the GDA Guidance to Requesting Parties (RP) (Ref. 7).
- Design Change Submissions proposed by Westinghouse which have been incorporated within the GDA scope with agreement of ND.

7 Within the Step 4 Plan the following generic HSE commitments were required to be taken into consideration as part of the Step 4 Internal Hazards assessment.

- Consideration of issues identified in Step 3.
- Judging the design against SAPs and judging whether the proposed design reduces risks As Low As Reasonably Practicable (ALARP).
- Inspections of the Requesting Party's procedures and records.
- Independent verification analyses.
- Reviewing details of the design controls, procurement and quality control arrangements, to secure compliance with the design intent.
- Establishing whether the system performance and reliability requirements are substantiated by the detailed engineering design.
- Assessing arrangements for moving the safety case to an operating regime.
- Assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final design, building and construction.
- Judging whether significant site parameters are appropriately defined in the generic site envelope.
- Reviewing overseas progress and issues raised by Overseas Regulators.
- Considering unresolved issues raised through the public involvement process.
- Resolution of identified nuclear safety issues, or identifying paths for resolution.

2.2 Standards and Criteria

8 The relevant standards and criteria adopted within this Step 4 assessment are primarily the Safety Assessment Principles (SAPs), internal technical assessment guides, relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant Technical Assessment Guides (TAGs) have been detailed within this section. National and international standards and guidance have been referenced where appropriate within the assessment report. Relevant good practice, where applicable, has also been cited within the body of the assessment.

2.2.1 Safety Assessment Principles

9 The key SAPs applied within the Internal Hazards Assessment of the AP1000 are included within Table 1 of this Assessment Report.

2.2.2 Technical Assessment Guides

10 The following TAGs have been used as part of this assessment:

- Technical Assessment Guide - Internal Hazards, T/AST/014 Issue 02 (Ref. 8).
- Technical Assessment Guide – Diversity, Redundancy, Segregation and Layout of Mechanical Plant, T/AST/036 Issue 02 (Ref. 9).
- Technical Assessment Guide – Guidance on the Purpose, Scope and Content of Nuclear Safety Cases, T/AST/051 Issue 01 (Ref. 10).

2.2.3 National and International Standards and Guidance

11 International standards and guidance have been used as part of this assessment. The following standards have been used to inform my assessment:

- *Safety of Nuclear Power Plants: Design. Safety Requirements*, NS.R.1(Ref. 11).
- *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants*. Safety Guide, NS.G.1.7 (Ref. 12).
- *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants*. Safety Guide, NS.G.1.11 (Ref. 13).
- *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels*. Issue S: Protection Against Internal Fires, (Ref. 14).

2.3 Assessment Scope

12 The intended assessment strategy for Step 4 for the internal hazards topic area was set out in an assessment plan that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below:

2.3.1 Findings from GDA Step 3

13 A number of areas were identified during Step 3 that warranted further assessment within Step 4. These were related to a lack of detail claims and arguments that would have been expected as part of the scope of the PCSR, submitted in support of Step 3 assessment. In addition, from the limited sampling undertaken by ND during Step 3 due to resource and time implications, further areas have been identified for assessment during Step 4. The areas identified for further assessment are detailed within Table 2, below:

Table 2: Areas for Further Assessment Identified Within Step 3

Assessment Area	Description
Hazard Barrier Qualification	Assessment of the arguments and evidence associated with the justification and adequacy of the fire barriers.
Fire Protection System (FPS)	Further assessment of the claims, arguments and evidence for FPS installed as part of the AP1000 that are currently claimed for nuclear safety.

Assessment Area	Description
Hazard Barrier Qualification	Assessment of the arguments and evidence associated with the justification and adequacy of the fire barriers.
Defence-in-Depth	Assessment of the defence-in-depth (prevention, limiting severity and limiting consequences).
Operator Actions	Operator actions are to be the subject of further detailed assessment as there remains uncertainty over what potential actions may be required for less significant yet more frequent events coupled with a need to clarify what operator recovery actions are envisaged >72 hours after the event in relation to facilitating access.
EMI	Assessment of the potential sources of EMI.
Internal Hazards Topic Report	Assessment of the AP1000 Internal Hazards Topic Report produced as a key supporting reference to the PCSR.
Exceptions to Segregation	Whilst in principle, the approach to the segregation of Systems Structures and Components (SSCs) important to safety is consistent with UK expectations, further assessment of the detailed claims, arguments and evidence is to be undertaken.
Categorisation and Classification	Assessment of the WEC AP1000 categorisation and classification document.
Internal Flooding	Further assessment of the claims, arguments and evidence associated with internal flooding is to be undertaken.
Dropped Loads and Impact	As there has been limited assessment of dropped loads and impact during Step 3 further assessment of the potential hazards associated with dropped loads and impact is to be undertaken.
Internal Missiles	Due to a lack of detailed claims and arguments associated with the potential for missiles to occur both inside and outside containment further assessment is required.
Internal Explosion	Further assessment to determine whether there are any nuclear safety claims associated with potential explosions arising from flammable liquids or gases is to be undertaken.
Pipe whip	The methods used to protect against pipe whip in this case are consistent with the approaches taken within the existing UK fleet e.g. distance, barriers and restraints, however, further assessment is to be undertaken during Step 4 to identify the areas where additional protection is installed to ensure that safe shutdown is assured and that the designation of such areas and protection is adequate.
Internal Hazards – General	Sampling of the evidence provided to support the claims and arguments made during Step 3.

2.3.2 Additional Areas for Step 4 Internal Hazards Assessment

14 There were no additional areas for assessment identified within Step 4 that had not first been raised during Step 3.

2.3.3 Use of Technical Support Contractors

15 As part of the assessment undertaken during Step 4, two separate pieces of work were undertaken by Technical Support Contractors (TSC) associated with internal hazards. Atkins undertook an assessment of internal fire, explosion and missile, while Frazer Nash undertook assessment which included pressure part failure, dropped loads and impact, and internal flooding. The assessment undertaken was based upon Revision 1 of the Internal Hazards Topic Report (Ref. 15) issued to ND in February 2010. It is recognised that this version of the topic report was revised in September 2010, however, the information contained within the assessment undertaken by both TSCs was provided to Westinghouse to inform the future revision. I have included some of the main conclusions from the assessments undertaken specifically within the Sections 4.1 and 4.2 of this report. As the assessments are based upon Revision 1 of the Internal Hazards Topic Report, I believed it made this assessment report clearer if I included the conclusions of the TSC assessment at the start of my assessment report, as my detailed assessment is based upon the PCSR that should have addressed all the concerns arising from the TSC assessment that was undertaken.

16 The assessment reports produced by the TSCs were used to inform my regulatory judgements only; I was not directed or obliged to accept or otherwise information presented by the TSC. Use of their work was entirely at my own discretion, and I have made my decisions and reached the judgements presented in this report based on a number of factors, including the work offered by my TSCs.

2.3.4 Cross-cutting Topics

17 There were a number of areas during the Step 4 assessment when there was a need to consult with other assessors. These areas have been overseen by ND to ensure that all potential interactions are captured and that nugatory duplicate assessment work is prevented. The cross-cutting topics within the Internal Hazards Assessment of AP1000 were:

- Categorisation and Classification
- Civil Construction and Substantiation of Module Design against internal hazards.
- Operator Actions associated with internal hazards
- Electro-Magnetic Interference
- Dropped Loads and Load Mishandling
- Fault Schedule and Deterministic Analysis
- Probabilistic Safety Analysis

2.3.5 Integration with Other Assessment Topics

18 The following table identifies the key assessment areas involved in an integrated approach taken to the cross-cutting subjects associated with internal hazards (other technical areas were consulted during the assessment process as appropriate):

Cross-cutting Subject	Specific Assessment Area	Technical Assessment Area
Categorisation and Classification	All Internal Hazards	All assessment disciplines overseen by Unit Heads
Civil Construction / Module Design for Internal Hazards	Internal Flooding Internal Fire Pipe whip/Jet Impingement and Steam Release Missile/Impact	Civil Engineering
Operator Actions	Internal Fire Internal Flooding	Human Factors
Electro-Magnetic Interference	Electro-Magnetic Interference	Electrical Assessment Control and Instrumentation Assessment
Dropped Loads and Impact	Dropped Loads and Impact	Mechanical Engineering Assessment Civil Engineering Assessment Control and Instrumentation Assessment
Fault Schedule and Deterministic Analysis	Redundancy, diversity and segregation for Internal Hazards.	Deterministic Safety Assessment
PSA	Internal Fire Internal Flooding Dropped Loads and Impact Pipe whip/Jet Impingement and Steam Release	Probabilistic Safety Analysis

2.3.6 Out of Scope Items

19 There are no out of scope items within the AP1000 Step 4 Internal Hazards Assessment.

3 REQUESTING PARTY'S SAFETY CASE

20 Revision 2 of the Internal Hazards Topic Report (Ref. 16) is a supporting reference to Revision A of the PCSR (Ref. 1) and provides detail analysis of the internal hazards considered. It provides information on the method by which internal hazards are identified, the process applied in the assessment of internal hazards, and the claims, arguments and evidence to protect the plant against the effects of the identified internal hazards. Chapter 11 of the PCSR captures the findings of the Internal Hazards Topic Report and its supporting references. The European Design Control Document (EDCD) (Ref. 19) is referred to in both the PCSR and the Topic Report as a source of further detailed information relating to internal hazards.

21 The Internal Hazards Topic Report defines internal hazards as, *"….those hazards to plant, structures and personnel that originate within the Licensee's site boundary but are external to the reactor system. That is, hazards of which the Licensee has control over the initiating event in some form."*.

22 The hazards specifically addressed within the PCSR are:

- Internal fire.
- Internal flooding.
- Pressure part failure.

- Internal explosions.
- Internal missile.
- Release of toxic, corrosive or flammable material.
- Dropped loads and load mishandling.
- Biological agents.
- On-site transport.
- Electro-Magnetic Interference (EMI).

23 The PCSR provides details of the scope, basis and content of the internal hazards safety case. It is stated that the assessment is a Design Basis Accident (DBA) assessment which only considers reasonably foreseeable faults and not severe accident analysis. It does not consider initiating events less frequent than 1×10^{-7} per year or fault sequences with initiating events less than 1×10^{-5} per year.

24 Chapter 11 of the PCSR addresses internal hazards from a solely deterministic approach i.e. a hazard such as fire is assumed to occur and response and tolerance of the plant to it is assessed with no consideration of frequency. The only exception to this is associated with simultaneous independent internal hazards which are not addressed as they are considered to be less frequent than the criteria mentioned in the previous paragraph.

25 All normal modes of operation are considered and an internal hazard is assumed to occur simultaneously with the most adverse normal plant operating state or configuration e.g. during outages and maintenance periods. Furthermore, the application of the single failure criterion is included within the safety case where applicable.

3.1 AP1000 Approach to Safety

26 The PCSR provides details of the AP1000 approach to safety. The approach is that passive safety systems provide the principal means of delivering Category A safety functions – any function that plays a principal role in ensuring nuclear safety. These passive Systems Structures or Components (SSCs) are classified as Class 1 and can, alone, mitigate Design Basis Accidents (DBAs) and meet Probabilistic Risk Analysis (PRA) safety goals.

27 The Class 1 safety systems use “passive” processes and include dedicated safety systems which are not normally used for normal operation.

28 Systems containing Class 1 equipment that function to mitigate DBAs have components redundancy so that their Class 1 safety-related functions can be performed even in the unlikely event of the most limited single failure occurring coincident with the postulated DBA.

29 In addition Class 1 or Class 2 SSCs reliably support normal operation and/or prevent unnecessary actuation of the accident mitigation Class 1 systems by responding to fault conditions and restoring the plant to a safe condition minimising the challenge on Class 1 systems. They provide an additional layer of defence which is termed and claimed as defence in depth.

30 Some of the Class 1 SSCs activate as required in response to the fault situation and deliver their safety function for as long as is required or until they have fulfilled their

function. Others necessarily have a limited capacity such as the batteries, the Passive Containment Cooling Water Storage Tank (PCCWST) and the Main Control Room (MCR) Emergency Habitability System. Where this is the case the AP1000 design ensures that these capacities are sufficient to deliver the safety function using these systems for 72 hours. This 72 hours period is embodied within the definition of a Category A safety function. These 72 hours Class 1 functions can be extended by a limited number of post 72 hour functions that are defined as Category B functions and their delivery is provided by or supported by a limited set of Class 2 SSCs. The safety case will need to demonstrate that these safety functions can be maintained until the plant does reach a safe and stable state in all cases beyond 72 hours.

31 So far as internal hazards are concerned, the safety case must demonstrate that an internal hazard within the design basis cannot both initiate a fault and prevent the delivery of the safety function that respond to that fault. Failure of the safety system on its own as a result of an internal hazard – i.e. the hazard does not also cause a reactor fault – would just require the reactor to be shut down and reach the safe shutdown state and provided this is not prevented by the consequences of the initial event then safety can be ensured. If the initiating event just causes the failure of the duty systems but not the safety systems then the safety systems will respond to the fault as intended.

32 Since the passive Class 1 SSCs used for DBA mitigation are not used in normal operation and on their own can mitigate DBAs, the safety case can be made by demonstrating protection of Class 1 SSCs from internal hazards such that they can still deliver their safety function. It also has to demonstrate that post 72 hours, the limited set of Class 2 SSCs that may be required to support the Category A safety functions are adequate and available.

33 An overview of the case for each of the internal hazards is provided within the following sections.

3.2 Summary of the Internal Hazards Safety Case Presented in PCSR

34 The following sections provide summaries of the salient points raised within the PCSR for each internal hazard.

3.2.1 Internal Fire

35 The PCSR approach to internal fire hazards is to demonstrate that any postulated internal fires within the design basis do not prevent the delivery of the Category A safety functions and the supporting Category B safety functions and is demonstrated through either:

- The SSCs being qualified to withstand the internal fire hazard; or
- The provision of sufficient redundant trains providing the nuclear safety functions and that the trains are segregated from each other such that and any credible internal fire will not prevent delivery of the Category A or the Category B supporting functions; or
- The SSCs are segregated from areas containing significant fire hazards.

36 In addition, the approach involves the assessment of the consequences of fire and requires that combustible loads are reduced so far as is reasonably practicable.

37 Within the design of AP1000, fire hazards are minimised and controlled through the specification of appropriate materials of construction, the identification and minimisation

of fire loading, control of ignition sources, and through the segregation of fire loads from areas containing Class 1 SSCs.

3.2.1.1 Segregation

38 In areas outside of containment, the plant is segregated into fire compartments composed of one or more rooms within a plant area. Due to limitations on equipment positioning and routing, and the requirements of the Passive Containment Cooling System (PCS), the containment building consists of just one compartment that encompasses the entire building.

39 In the containment building, fire spread is prevented by provision of adequate separation of equipment by distance or height, in particular redundant trains of safety systems, and by the use of passive fire protection features to separate redundant Systems, Structures and Components (SSCs) such as the Automatic Depressurisation System (ADS) valve stage 1, 2 and 3 valves and cables from different electrical divisions (B and D Penetration Room).

40 To prevent the spread of fires, passive fire protection measures such as fire resistant barriers and physical or spatial separation are used in the fire protection design of AP1000.

41 Fire compartmentalisation is used extensively throughout AP1000. The walls, floor and ceiling of fire compartments in the Nuclear Island are surrounded by fire resisting barriers. The fire barriers are constructed to withstand the complete combustion of the fire load within the enclosure (full room burn out) thereby preventing the fire from propagating across to, or otherwise causing direct or indirect damage to, materials or items on the side of the fire barrier that are not exposed to the fire. This prevents the effects of a fire in one compartment from damaging redundant SSCs located in adjacent fire compartments. Fire areas within the Nuclear Island are all 3 hour fire compartments, except for the Main Control Room (MCR) where the ceiling is not a fire barrier; instead the floor of the room above (VBS MCR/C&I equipment room) provides adequate 3 hour fire barrier protection against fire for the MCR below. These barriers are Class 1 SSCs. Although there are no Class 1 SSCs located outside of the Nuclear Island, many of the fire areas in these other buildings also form fire resistant compartments but these are not nuclear Class 1 barriers.

42 Primary fire compartment barriers protecting Class 1 SSCs are themselves Class 1 structures and are rated for load bearing capacity, integrity and insulation. Other fire barriers are fire rated for integrity and insulation only. The number of penetrations in fire compartment barriers including ventilation ductwork, cables and pipework, is minimised as far as possible. In all other fire compartments the fire resistance of fire barriers is specified based on the fire load and the calculated fire severity of the compartment. In specific instances where fire severity is estimated to be greater than three hours (wherever there is a significant oil inventory), a three hour barrier is specified and additional active fire protection systems are installed such that the barrier is not compromised. Such barriers occur within the turbine, annex and Diesel Generator (DG) buildings and do not occur within the Nuclear Island (NI). A fuel oil pool fire in these areas does not threaten the Category A safety function even in the event of the failure of the active fire protection systems to operate.

43 Penetrations are fire stopped to the same fire resistance (integrity and insulation) as the barrier they penetrate; this reduces the potential routes for the spread of fire and hot

gases. Fire dampers, and doors penetrating fire barriers are also fire rated for integrity and insulation from both sides will comply with the relevant parts of the appropriate standard. Combination fire and smoke dampers penetrating fire rated compartment walls will be similarly resilient and meet the single fault criterion; these are provided as a minimum at Class 1 fire barriers and on personnel escape routes.

44 Passive fire protection features are used to protect cable routes and ventilation ductwork of redundant systems from the effects of fire. For example a three hour fire rated ventilation ductwork enclosure/shaft is used to segregate the annex/auxiliary building Heating Ventilation and Air Conditioning (HVAC) systems as they enter and leave the north air handling equipment room in the annex building. Within the NI there are a number of cable ducts/chases protecting Class 1 IDS cables, including a three hour fire resistant enclosure for the Division B & D penetration room within the containment building.

45 The PCSR concludes that such provisions ensure that a fire is contained within the fire compartment of origin and does not threaten Class 1 SSCs located in other fire compartments.

3.2.1.2 Separation

46 Inside the containment building, fire compartmentation cannot be provided because of the need to maintain the free exchange of gases for purposes such as passive containment cooling. Instead, the containment building is a single fire area encompassing the entire building and is a 3 hour fire compartment. Fire zones are identified within this fire area that establish the zones of influence i.e. the extent to which a fire originating within any given location can spread and cause damage to equipment. Many of the fire zones (e.g. each of the stream generator rooms) have walls which are modular steel-concrete composite constructions and form significant physical barriers from other fire zones for much of their height.

47 Where the segregation of fire areas by a fire-rated full enclosure is not practicable for functional reasons, Class 1 SSCs are separated by distance (horizontal and vertical) to the maximum extent practicable and it is assumed that all SSCs within a fire zone fail as a result of fire in that zone. Fire barriers are incorporated where practicable to minimise fire spread beyond the fire zone via radiated and conducted heat. For example the redundant sets of the ADS Stage 1, 2 and 3 valves are stacked above the pressuriser and are separated from one another by more than 10m vertically and passive fire protection systems as well as by other plant and equipment. A fire disabling one set of valves in one fire zone does not spread to the vertically adjacent zone.

3.2.1.3 Redundancy

48 In the event of a fire within any fire compartment forming part of the AP1000 plant (or fire zone within the containment building), the PCSR pessimistically assumed that all SSCs fail within that area. In general, this might result in the safety function(s) supported by the equipment within that fire compartment no longer being delivered and / or spurious actuations that may have a negative impact on plant safety. The AP1000 plant is designed such that:

- No single SSC failure can result in the failure to deliver the Category A safety functions (taking into account that there is a periodic need to take certain individual systems offline during operation in order to undertake maintenance activities).

- No spurious activation can cause erroneous actions that may have a negative impact on plant safety.

3.2.1.4 Defence in Depth

49 The internal hazards nuclear fire assessment makes no nuclear safety claim on Class 2 systems that provide defence in depth for Category A safety functions, apart from those Category B safety functions required post 72 hours following an accident. The assessment pessimistically assumes that all such systems are unavailable and therefore the assessment identifies redundant Class 1 equipment in order to fulfil the safety function.

50 An example of this is the fixed fire fighting system which is not relied upon to protect Category A safety functions, however, it is used to protect Class 2 systems and reduce the demand on the Class 1 systems. There are seismic design requirements applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake. In addition, the containment isolation valves and associated penetration piping for the FPS are Class 1 and Seismic Category I. The FPS is not required to remain functional following a plant accident, or the most severe natural phenomena, except (as stated) following an earthquake.

3.2.1.5 Internal Fire Hazard Analysis

51 The analysis presented in the Internal Hazards Topic Report, which supports the PCSR, is an integral part of the process of selecting passive fire protection methods, ventilation and smoke control, fire detection, alarm and suppression systems, and provides a design basis for the fire protection system. The following assumptions used in the assessment of the design are:

- Design basis fire assumptions.
  - i) Only a single, independent fire is assumed to occur in any plant location.
  - ii) An independent fire is not assumed to occur simultaneously with the most severe natural phenomena, e.g. tornadoes, flooding or earthquakes or during other internal initiating events such as Loss of Coolant Accidents (LOCA) or loss of off-site power (LOOP).
  - iii) The fire is assumed to occur under worst case normal plant conditions for the initiating fire which may include such states as loss of a redundant train for maintenance purposes or under early shutdown conditions when the systems are pressurised.
  - iv) Fire spread to adjacent fire areas is only discounted where adequate fire resistant barriers (and their penetrations) appropriate to the fire hazard are provided.
  - v) Fire spread to adjacent fire zones within containment is only discounted where adequate fire separation and or passive fire protection features are provided.
  - vi) A design basis fire is a credible initiating event for other internal hazards such as explosions, floods or loss of offsite power.
- Consequential fires, generated as a result of other internal initiating events, such as explosions are considered credible.

3.2.1.6 Conclusions

52 The PCSR concludes that deterministic analysis of postulated, design basis, internal fire events shows that all Class 1 SSCs will continue to provide their Category A safety function following the worst case postulated internal fire, even in the presence of an unrelated single failure elsewhere in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function would be maintained by other, additional and redundant, Class 2 SSCs. In addition, other measures have been taken within the design of AP1000 that, although not claimed in the deterministic analysis, will further reduce the consequences of postulated internal fires such as the provision of active fire suppression systems in some areas.

53 The PCSR also concludes that since the Category A safety functions can be maintained despite internal fires, the safety of the plant is assured. The PCSR judges that only minimal safety benefit may result from the introduction of further design measures to reduce the risks further.

3.2.2 Internal Flooding

54 The PCSR section on internal flooding reflects Westinghouse's current position and understanding as based on the internal flood analyses that have been carried out to date. These calculations are preliminary and the results reported in this section may change as further analyses are completed.

3.2.2.1 Internal Flooding Hazard Analysis

55 The internal flooding hazard analysis demonstrates that the safety Class 1 SSCs are protected from flood sources, by distance and/or physical barriers. Postulated internal floods within the design basis do not prevent the delivery of the Category A safety functions and the post-72 hour Category B safety functions. Consideration of internal flood hazard sources in other locations is limited to the demonstration that the Nuclear Island (NI) is adequately protected from a flood from these sources, by distance and/or physical barriers.

56 The PCSR states that the potential for internal floods to cause significant damage to Class 1 SSCs is minimised, where practicable by:

- Limiting fluid inventories contained within the plant.
- Segregating Class 1 SSCs from areas containing significant flood hazards.
- Locating Class 1 SSCs above the maximum credible flood height that could arise following postulated flood hazards.
- Specifying, designing, constructing and maintaining Class 1 SSCs so that they will provide their safety function, if required, when fully submersed.

57 The PCSR also states that the threat to Class 1 SSCs, posed by postulated internal flooding events has been considered in the design. Protective measures taken against the flood hazard include:

- The location and mass of significant fluid inventories have been identified on site, and these are subject to change control.
- The site is graded such that any credible internal flood in other buildings cannot affect the Nuclear Island.

- Fluid retaining structures are appropriately designed, and will be constructed and maintained in accordance with their safety categorisation, to minimise the likelihood of failure and size of release.
- The potential for internal flooding effects has been reduced by minimising the volume of liquid available for release, i.e. the flood hazard source, especially in the non-radioactive portion of the auxiliary building that contains Class 1 SSCs, by:
  i) Eliminating water systems, with the exception of the FPS and Potable Water System (PWS).
  ii) Not locating potential sources of large volume, high capacity water systems (for example the SWS) in the NI.
  iii) Controlling the volume of fire protection water that can be released in the nonradioactive portion of the auxiliary building and containment so that unacceptable internal flooding is not possible.
- Drainage is provided that is:
  i) Designed and will be constructed and maintained specifically to protect against and/or mitigate postulated internal flooding events.
  ii) Does not require operator action to function to protect Class 1 SSCs.
- Where appropriate, walls, floors and ceilings (and any penetrations through them) are designed and constructed to withstand the loadings imposed on them by postulated internal flooding events, hence:
  i) Maintaining the claimed flow paths and
  ii) Preventing secondary damage to other Class 1 SSCs.
- Penetrations through identified barriers are designed and will be constructed and maintained to provide the same level of withstand capability as the relevant barrier.

58 The analysis presented in PCSR consisted of the following steps:

- Identification of credible sources (such as postulated pipe ruptures, pump mechanical seal failures, storage tank ruptures, actuation of fire suppression systems, and sources external to the compartment, including backflow through floor and equipment drains or drainage flow from other areas).
- Identification of essential equipment in areas.
- Determination of flow rates and flood levels.
- Evaluation of preliminary results on essential equipment.

3.2.2.2 Consequences of Postulated Internal Flooding Events

59 Having identified credible flood sources, the consequences of such events were then assessed to determine the maximum expected flood depth, initially without consideration of drainage and other potential flood protection / mitigation measures. Where SSCs were identified as potentially being affected by the maximum flood depth then further calculations were performed using more realistic, but still conservative, assumptions such as:

- Maximum flood rates and volumes, (e.g. double-ended guillotine breaks of pipework and catastrophic storage tank rupture and drainage).
- Coincidental failure of a single active component (single failure criterion) within any required systems used to mitigate the effects of the flooding event.
- Failure of equipment due to a common cause with the initiating event (including loss of offsite power).
- Unless specifically engineered for the purpose, no claim is made on the leak tightness of openings (e.g. doors) even if rated for other hazards (e.g. fire doors). Two cases have been considered in the analysis to determine the maximum flood level:
  i) In the room under consideration by assuming a zero gap under the door and no door opening under hydrostatic pressure.
  ii) In the adjacent rooms by assuming a gap under the door of 1.25 cm and that the door will open at its maximum design differential pressure of 0.03 MPa at the bottom of the door.
- There are watertight doors on the NI connecting rooms 12166 and 12167 to room 12169 on level 1 of the radiological auxiliary building.
- Fluid continues to flow down stairwells or into the stairwell preferentially through other doors.
- No credit is taken for operation of sump pumps to mitigate the consequences of flooding.
- For each storage tank rupture, it is assumed that the entire tank inventory is drained.
- Flooding affecting an item of non-Class 1 equipment is assumed to fail the whole system of which it is a part.
- Maximum flow rate levels (including the effects of stairwells, floor openings, and floor sleeves) are determined.
- Piping line properties such as line size, temperature, pressure, and source of flow (pump or tank) were obtained from various sources including:
  i) System Specification Documents (SSD).
  ii) System Process and Instrumentation Diagrams (P&IDs).
  iii) Process flow calculations.
  iv) Isometric drawings.

60 The current auxiliary building flooding analyses also incorporate risk mitigation assumptions regarding drain lines and operator actions during a flooding event. These are:

- Drain lines for the flooded regions are conservatively assumed to be 75% open, as stated in the Design Criteria for Floods.
- In one scenario, credit is currently taken for corrective action by the operator to terminate the flooding event 30 minutes after control room indication of flooding. However, this action is identified as a risk mitigation measure as the operator's failure to isolate the flooding source results in a reactor trip and does not affect the availability of the Category A safety functions.

3.2.2.3 Outcome of the Flooding Hazard Analysis

61 The PCSR states that the flooding hazard analysis has only been completed for the Containment Building and Shield Building. The results provided within the PCSR for the other buildings are indicative and as mentioned, previously, the PCSR recognises that these indicative results may change depending upon the outcome of the analysis.

3.2.2.4 Conclusions

62 The PCSR concludes that, based on design basis analysis of internal flooding events for the Shielding and Containment building, the Class 1 SSCs continue to provide their Category A safety function following the worst case postulated internal flood, even in the presence of an unrelated single failure elsewhere in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function can be maintained by other, redundant, Class 2 SSCs. In addition, other measures have been taken within the design of AP1000 that, although not claimed in the deterministic analysis, should further reduce the consequences of postulated internal floods.

63 The PCSR further concludes that only minimal safety benefit may result from the introduction of further design measures to reduce the risks further and would not warrant the disproportionate time, cost and trouble that would result.

64 It should be mentioned here that the analysis presented in the PCSR for the remaining areas are preliminary and potentially the results and the discussion presented within PCSR may change.

3.2.3 Pressure Part Failure

65 PCSR considers pressure part failure of pressurised components from pipes, vessels, tanks and heat exchangers which may result in failure of a train of the system associated with the pressurised component. In addition such an event may cause damage to other plant items due to hazard effects such as pipe whip, jet impingement, blast effect and compartment pressurisation, fluid spray, heating and condensation, flooding, missiles and water hammer. This section covers pipe whip, jet impingement, compartment pressurisation, spray, heating and condensation effects of pressure part failures.

3.2.3.1 Pressure Part Failure Hazard Analysis

66 The analysis of postulated pressure part failure demonstrates that the Safety Class 1 SSCs are protected from significant damage. Postulated pressure part failures within the Design Basis do not prevent the delivery of the Category A safety functions and the supporting Category B safety functions.

67 The potential for pressure part failures to cause significant damage to Class 1 SSCs is minimised, where practicable, by:

- Minimising the potential sources, locations and/or consequences of postulated pressure part failure, and;
- Locating Class 1 SSCs outside of the zone of influence of any postulated pressure part failures that are deemed credible, or;

- Providing protection to any Class 1 SSCs that may be located within the zone of influence of a postulated pressure part failure that is deemed credible or;
- Qualifying any Class 1 SSCs that may be located within the zone of influence of a postulated pressure part failure so that it continues to provide its Category A safety function in the applicable environmental conditions.

68 The arguments presented in PCSR, in support of the Design Basis for pressure part failures, inside containment differ slightly from that for failures outside containment.

Inside Containment

69 Within containment, Class 1 SSCs are not separated and segregated by barriers to the same extent as Class 1 equipment outside containment because within containment they are connected to the primary circuit. The frequency and consequences of pressure part failures within containment are minimised by application of design features that reduce the possibility of a pressure part failure and then mitigate its consequences should failure occur. The following approaches are applied;

- The design and qualification of high pressure SSCs within the containment.
- A combination of separation and use of barriers to minimise the potential to affect Class 1 SSCs.
- Quantification of SSCs to operate under harsh environmental conditions (water spray, steam, over-pressure).

70 In addition it is argued that it is not credible for there to be a high energy failure mode for a limited set of AP1000 pipework. This covers selected pipework from the following systems:

- Reactor System.
- Reactor Coolant System (RCS).
- Residual Heat Removal System.
- Steam Generator (SG) - Main Steam Line.

Outside Containment

71 Outside of containment a failure of a pressurised system has been conservatively assumed to lead to the loss of all the equipment within a room in the same way as has been assumed for internal fire. As is shown for internal fire when this assumption is made it can still be shown that the Category A safety functions will be delivered. Additionally, the effects of a pressure part failure are limited to a single room through the use of structural barriers.

72 Where pipe whip has the potential to cause the failure of a Class 1 SSC then mitigations have been provided in the form of restraints, shielding, barriers and separation.

73 The analysis presented in PCSR consisted of the following steps:

- Identification of hazard sources, including consideration of:
  i) Postulated ruptures.
  ii) Leak-before-break.
  iii) No break zones.

- Evaluation of effects on equipment, including:
  i) Hydraulic transients, pipe whip, jet effects and protective hardware.
  ii) Operability of safety classified systems and components.
  iii) Environmental effects.
  iv) Sub-compartment pressurisation.

3.2.3.2 Consequences of Postulated Pressure Part Failure

74 Having identified credible pressure part failures, the consequences of such events were then assessed. The consequences of ruptures are analysed for dynamic effects (pipe whip, hydraulic transients, jet impingement, and compartment pressurisation), operability and environmental effects on Class 1 SSCs. The post-rupture harsh environment assessment covers:

- Spray wetting effects.
- Environmental effects (rupture-induced pressure, steam, corrosivity, combustibility, radiation, chemical spills).
- Temperature and humidity effects.

75 The PCSR presented the principal conclusions of the pipe break hazard analysis for the following areas:

- The containment and shield buildings.
- The clean auxiliary building.
- The radiological auxiliary building.
- Buildings adjacent to the NI.
- Areas outside the NI.

3.2.3.3 Containment/Shield Building

76 The PCSR states that in the following areas the potential for pipe whip cannot be precluded and hence Class 1 SSCs contained in them are protected against pipe whip by pipe whip restraints or barriers or shields.

- ADS valve areas.
- SG compartments.
- Upper pressuriser compartment.
- Maintenance floor and mezzanine level.
- Pipe chase to Chemical Volume and Control System (CVS) Equipment Room.

77 With regard to potential sources water spray inside the Containment/Shield building, the PCSR identifies the following:

- RCS, including the:
  i) Reactor vessel.

ii) Pressuriser.
iii) Reactor coolant pumps.
iv) Steam generator channel heads.
v) Associated piping and valves.

- The Steam Generator System (SGS), including the:
  i) In-Containment Refuelling Water Storage Tank (IRWST).
  ii) Accumulator tanks.
  iii) The Core Make-up Tanks (CMT).
  iv) Passive Residual Heat Removal (PRHR) system heat exchanger.
- ADS.
- Normal Residual Heat Removal System (RNS).
- CVS.

78 The PCSR states that Class 1 SSCs are designed to withstand being subjected to water spray while the majority of other SSCs will also withstand being subjected to water spray. The PCSR also identifies areas containing redundant Class 1 equipment which have been qualified to withstand water spray without loss of operability. Barriers also prevent spray affecting the redundant Class 1 equipment.

79 SSCs in the following areas are also identified to withstand steam release without loss of operability.

- Operating Deck and Refuelling Cavity.

  The safety-related equipment in this location is:
  i) Class 1 cable trays.
  ii) Class 1 electrical penetrations.
  iii) SG 1 narrow range level.
  iv) SG 2 narrow range level.
- ADS valve areas.
- SG compartments.
- Vertical access and RCDT room.
- Maintenance areas.
- Passive core cooling system compartments.
- Reactor Containment Boundary.

80 The PCSR states that equipment within the containment that is required to operate after a postulated DBA is qualified for the steam conditions that will be present. The equipment qualification and testing programme will ensure that the equipment specified and fitted to the AP1000 meets requirements.

81 With regard to overpressure, the PCSR considers postulated pressure part failure that may occur in the SG compartments. The boundaries of the room are, however, designed

to prevent this affecting the redundant SSCs in the other SG compartment or SSCs in the adjoining RCS loop compartment, and a reference is made to the AP1000 Barrier Matrix.

3.2.3.4 Clean Auxiliary Building

82 The clean auxiliary building is potentially subject to pipe whip, water spray and steam release hazards from a variety of potential sources, including:

- SSCs in the Main Steam Isolation Valve (MSIV) compartments (main and start-up feedwater lines, feed and main steam lines).
- SSCs in the mechanical equipment room.
- SSCs in the valve/piping penetration compartment.

83 The auxiliary building contains radiologically controlled and non-radiologically controlled (clean) areas that are physically separated by structural walls and floor slabs. These structural barriers, and the associated penetrations, are designed to prevent the effects of postulated pressure part failures within one part of the building from damaging Class 1 SSCs contained within the other half.

84 The areas within the clean auxiliary building that contain these hazard sources are addressed in turn in the following text.

Main Steam Isolation Valve Compartments

85 Each compartment comprises a feed main, a start feedwater line, a steam main, steam isolation valves, a power-operated atmospheric relief valve, six safety valves, and heating and cooling equipment.

86 The AP1000 Barrier Matrix demonstrates that the walls of the MSIV compartments are sufficiently robust that an impact arising from pipe whip of a main steam or feed line would not result in damage to SSCs delivering safety functions elsewhere in the auxiliary building. In addition, the compartment walls will also prevent the spread of steam or water from steam releases or water spray incidents from affecting the remainder of the clean auxiliary building.

87 Within these compartments, protection of sensitive components (the valve actuation cables) is provided in the form of barriers, deflectors or shields, to obviate the possibility of pipe whip induced failure or steam release (and related water spray).

88 Should a pipe whip or steam release (and related water spray) damage cabling within the MSIV compartments then the power-operated atmospheric relief valves may be inhibited. However, there are six spring-loaded steam safety valves that would operate as they require no electrical actuation signal. This would vent steam via an approved route away from safety Class 1 SSCs.

Mechanical Equipment Room

89 The mechanical equipment room contains containment isolation valves for the Component Cooling Water (CCS), demineralised water transfer and storage system, the FPS and ancillary lines to the SGSs.

90 The PCSR states that a pipe whip from the SG ancillary systems, or a steam release from the SG ancillary line is not expected to damage the remaining mechanical components within the mechanical equipment room, as they are constructed of high quality materials, designed to appropriate codes and standards and designed for their

operational environment with substantial margin and a Reference to AP1000 Barrier Matrix made.

91 Protection of the valve actuation cables is provided in the form of barriers, deflectors or shields, to obviate the possibility of steam release-induced failure. However, the isolation valves are generally fail-safe if the actuation cables are damaged.

Valve and Piping Penetrations

92 The valve and piping penetration room at elevation 100 ft (100' 0") contains automatically actuated containment isolation valves for the central chilled water system, PCS and demineralised water transfer and storage system.

93 A pipe whip from the PCS is not expected to damage the remaining mechanical components within the mechanical equipment room as they are constructed of high quality materials, designed to appropriate codes and standards and designed for their operational environment with substantial margin and contain low temperature fluid.

94 Protection of sensitive components (the valve actuation cables) is provided in the form of barriers, deflectors or shields, to obviate the possibility of pipe whip-induced failure. In addition, the isolation valves are generally fail-safe if the actuation cables are damaged.

95 The valve actuation cables in the valve / piping penetration room are qualified against the effects of a water release induced failure.

3.2.3.5 Radiological Auxiliary Building

96 The radiological auxiliary building is potentially subject to pipe whip, water spray and steam release hazards from a variety of potential sources, including; Component cooling water, central chilled water, hot water heating system, SFS, RNS, CVS and VES.

97 System failures due to pressure part failures are considered to be bounded by the overall conclusion reached for internal fire, as internal fires assume that all systems within an affected area are lost.

98 The auxiliary building contains radiologically controlled and non-radiologically controlled (clean) areas that are physically separated by structural walls and floor slabs. These structural barriers, and the associated penetrations, are designed to prevent the effects of postulated pressure part failures within one part of the building from damaging Class 1 SSCs contained within the other half. Further details are provided in the AP1000 Barrier Matrix.

99 The PCSR considers the following areas that contain hazard sources:

- Normal residual heat removal system pumps, heat exchangers and containment isolation valves.
- Containment isolation valves
- Habitability system compressed air tanks.

100 Other areas assessed within the PCSR include the following:

- Buildings adjacent to Nuclear Island including the Turbine Building and other Buildings and Structures.
- Areas outside the Nuclear Island.

101 The plant arrangement is based on maximising the physical separation of redundant safety Class 1 components and systems from each other and from other SSCs as appropriate. Therefore, in the event a pipe failure occurs, there is a minimal effect on other Class 1 systems or components required for safe shutdown of the plant or to mitigate the consequences of the failure.

102 Protection against the dynamic effects of pipe failures is provided by physical separation of systems and components, barriers, equipment shields, and pipe whip restraints. The precise method chosen depends largely upon considerations such as accessibility and maintenance.

103 The preferred method of providing protection is by separation. When separation is not practical, pipe whip restraints are used. Barriers or shields are used when neither separation nor pipe whip restraints are practical. This protection is not required when piping satisfies leak-before-break criteria.

3.2.3.6 Conclusions

104 The PCSR concludes that, based on deterministic analysis of the effects of postulated pressure part failures, the Class 1 SSCs would continue to provide their Category A safety function following the worst case event, even in the presence of an unrelated single failure else where in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function would, for the less severe events, be maintained by other, additional and redundant, Class 2 SSCs.

105 The PCSR judge that the time, trouble and cost associated with the introduction of additional safety measures to prevent or protect equipment from the secondary effects of pressure part failures is disproportionate to the minimal safety benefit that may result.

3.2.4 Internal Explosion

106 The PCSR considers internal explosions due to plant processes, equipment and materials including materials stored for subsequent plant use. The following type of contributory acts are considered:

- Incorrect location or storage of explosive materials.
- Accidental release of explosive materials (hydrogen) during conduct of operations.
- Accidental failure to control (ventilation system) accumulation of potentially explosive materials generated by operating processes.
- Development or creation of a detonation source under the same circumstances as when an explosive concentration of material is present.

3.2.4.1 Safety Design Approach to Internal Explosions

107 The design approach against internal explosions is presented in the PCSR as follows:

108 The potential for internal explosions to cause significant damage to SSCs is minimised by limiting and controlling explosive gas inventory of the plant, by design, construction, operation and maintenance of components containing potentially explosive material, and by segregating SSCs from areas containing explosive materials.

109 The quantity of potentially explosive material required for normal operating processes by the AP1000 design has been identified and storage facilities have been sized to minimise the severity of explosions that could occur. Safe distances for the storage facilities from the containment and auxiliary buildings have been determined, such that the maximum resulting explosive overpressures will not damage the structure and hence the SSCs protected by the structure.

110 Where explosive materials are required within buildings containing SSCs, the quantity available to be released in any leak is minimised by design. The volumes into which leaks could arise are sufficiently large that the LFL will not be reached. Except where it is necessary to supply explosive material to an SSC, the sites of potential leaks are separated and segregated from areas containing SSCs by structures designed to be sufficient to contain the effects of credible explosions.

111 Hydrogen is required within the turbine building as a coolant for the generators. It is sourced from the hydrogen storage tank located in the Plant Gas System (PGS) storage area outside and away from the west side of the turbine building. The areas which the pipe passes through are large enough that if an entire cylinder were to be released from a leak, the hydrogen concentration would be below the LFL of 4%. Additional protection is provided since the areas are also ventilated.

112 Hydrogen is also supplied from the high pressure storage cylinders to the Chemical and Volume Control System (CVS) within the containment. The supply line does not pass through compartments containing Class 1 and Class 2 equipment. The compartments through which the line passes are ventilated, and are large enough that release of a complete cylinder would not reach the LFL.

113 The hydrogen supply line is routed as far away as practical from potential ignition sources so that the chances of igniting any leak are reduced.

3.2.4.2 Control of Flammable Gas

114 The potential for internal explosions to cause significant damage to SSCs is minimised by engineered systems designed to control the flammable concentration of the gas. These include the ventilation and hydrogen re-combiners.

115 The five Class 1 battery rooms in the clean auxiliary building are ventilated mechanically. The ventilation is sized so that at the maximum hydrogen generation rate, the hydrogen concentration does not exceed 1%. The battery chargers are not interlocked with the exhaust fans or with the flow sensor and therefore, the chargers do not automatically stop charging if the airflow is stopped. There also is a hydrogen detector in each battery room. These detectors would not automatically shut down the charger, since the hydrogen detectors are not currently part of the Heating, Ventilation and Air Conditioning (HVAC) system. Procedures would direct, however, the operators to confirm that battery charging has stopped if the ventilation is lost to a battery. An explosion in one of these battery rooms should not affect any of the other battery rooms so back up power will be available and there would be minimal disruption to the operation of the plant.

116 The turbine building and annex building contains a battery charger and battery rooms. The ventilation arrangements are the same as for the auxiliary building battery rooms. Hydrogen detection is also provided in the turbine building. The battery rooms are segregated from each other and from the defence in depth Class 2 SSCs and the Class 2 equipment in the turbine building / annex buildings which support Category B safety functions. There are no Class 1 SSCs in the turbine building.

3.2.4.3 Redundancy, Separation and Segregation

117 The PCSR states that sufficient redundancy and segregation in the design and location of the SSCs ensure that the Category A safety function can be maintained in the worst, normally permitted, plant line-up despite loss of those SSCs affected by the explosion and in the presence of a credible unrelated single failure within the other SSCs.

118 Where an SSC supporting a Category A safety function can be affected by an internal explosion (e.g. the explosive material is supplied to the SSC so a leak could affect it), the PCSR assumes that the whole train is disabled, together with any other SSC at that location. The Category A safety function can still be provided by a redundant train protected by construction sufficiently robust to contain an explosion involving the maximum design quantity of explosive material.

119 The internal walls are of robust construction, in order to perform their structural functions and achieve their required fire resistance ratings. They therefore provide some protection against the effects of internal explosions. The rooms to which hydrogen is supplied are sized to ensure that the maximum possible hydrogen release, dispersed throughout the room, is below the LFL. Unavoidable permanent potential ignition sources within the rooms (e.g. electrical motors) are sited so that they are outside the potentially explosive region which might form during the largest potential hydrogen leak. Management controls prevent temporary potential ignition sources from being present in the potentially explosive region, thereby ensuring that a leak does not lead to an explosion. In the event of a leak combining with a failure of procedural controls, separation of redundant also provides protection from potential internal explosion. Maintenance and/or operating procedures would require explosive monitoring where activities that could potentially introduce them in any work area are undertaken. Local monitoring would help to preclude flammability and / or explosions.

3.2.4.4 Further Mitigation

120 The PCSR states the following further mitigation measures against the internal explosions hazards.

- Only the quantities of potentially explosive materials necessary for operations are provided on site.
- Where relatively large explosive quantities are required to be stored, these are located away from the buildings, at distances determined to be safe. An exclusion zone for structures near the liquid hydrogen storage facility has been determined to prevent any ignited release from progressing to a detonation.
- Smaller quantities of potentially explosive materials are stored closer to where they are required. The locations have been determined to be safe with regard to the NI.
- Piped hydrogen within the buildings is supplied from limited supplies, has a limited flow rate and passes through rooms sized or ventilated so that release of the maximum amount possible will not reach the LFL.
- Potential ignition sources (permanent and temporary) are not permitted near enough to the hydrogen supply line that they would be in the temporary potentially explosive region caused by a leak.

- Only Class 1 or Class 2 equipment which is supplied by hydrogen is close enough to any potential leak site to be damaged by an explosion.
- Redundant Class 1 and Class 2 equipment is located elsewhere, for fire separation reasons, which also has the effect of protecting the redundant equipment from explosions.
- The battery rooms are ventilated so that hydrogen generated by charging does not exceed 1%.
- Where processes may generate hydrogen, there are ventilation systems, hydrogen levels are monitored by fixed equipment, and equipment which can potentially be affected has segregated redundant equipment.

3.2.4.5 Conclusions

121 The PCSR conclude that the AP1000 risks associated with internal explosion are kept ALARP.

3.2.5 Internal Missiles

122 The PCSR considers internally generated missiles from pressurised components, rotating machinery, explosions or dropped loads.

3.2.5.1 Safety Design Approach to Internal Missiles

123 The consequences of missile generation are mitigated through the provision of segregation barriers that can withstand the impact of possible missiles such that the Category A safety functions and post-72 hour Category B safety functions are not compromised. Additionally redundant safety equipment is segregated by distance from the missile source.

124 The civil engineering structures provide structural support to the SSCs, but also act as suitable barriers for a number of functions including the prevention of accidentally generated missiles from travelling to a location where significant harm could occur. Civil structures that make up the NI are designated as Class 1. They are also Seismic Category I and are designed to resist tornado wind loads and remain functional when subject to tornado generated missiles. Seismic Category 1 structures can sustain local missile damage (partial penetration and local cracking or permanent deformation or both) provided that structural integrity is maintained and Class 1 SSCs are not subject to damage by secondary missiles, such as from concrete spalling.

3.2.5.2 Internal Missiles Hazard Analysis

125 The PCSR considers the following potential sources of internally generated missiles:

- Turbine disintegration.
- Rotating components.
- Pressurised components.
- Explosions.

- Falling objects and secondary missiles.

126 The PCSR presents qualitative arguments against the above sources.

3.2.5.2.1 Turbine Missiles

127 The missiles from a turbine failure are divided into two groups: “high trajectory” missiles which are ejected upwards through the turbine casing and may cause damage if the falling missile strikes a system or component, and “low trajectory” or “direct” missiles which are ejected from the turbine casing directly towards systems or components.

128 The turbine is oriented so that its shaft axis is perpendicular to the NI in which all of the Class 1 SSCs are located. The orientation of the turbines is such that any low or high trajectory missiles generated are most likely to be ejected perpendicular to the axis of the turbine. The probability that a missile is directed away from the perpendicular decreases as the angle to the turbine axis decreases. Hence, it is extremely unlikely that fragments resulting from turbine disintegration would strike the NI structures. Class 1 SSCs are located outside of the low trajectory missile strike zone.

129 The potential for missiles to be generated from the turbine is minimised by design. Turbine over speed protection systems are incorporated into the design. Turbine rotor integrity is provided by the integrated combination of material selection, rotor design, fracture toughness requirements, tests, and inspections. This combination results in a very low probability of a condition that could result in a rotor failure.

130 Class 1 SSCs are not located outside the NI (i.e. within the turbine, annex, radioactive waste or DG buildings). Class 2 SSCs are located both within the NI and in other structures of the AP1000. In order for any missile generated by turbine failure to impact Class 1 SSCs it must, as a minimum, penetrate the auxiliary building walls or the shield/containment buildings. The size and energy of turbine missiles (low or high trajectory) are bounded by those considered in the assessment for wind generated missiles covered by the external hazards assessment. If multiple missiles are considered, it is judged that the protection provided by the NI buildings will be sufficient to protect Class 1 SSCs.

3.2.5.2.2 Rotating Components

131 Rotating equipment comprises pumps, fans, motors and motor operated valves. Rotating equipment is designed with surrounding housings to contain fragments in the event of failure i.e. the energy of rotating parts will be contained. Rotating components are protected against excessive over speed where appropriate, thus, minimising the likelihood of disruptive failure. In addition, material characteristics, inspections, quality control during fabrication, erection and prudent operation contribute to reduce the likelihood of missile generation.

132 The potential consequences of a failure of rotating equipment can be summarised by considering the initial failure and then the result of any impact of a missile. Inside the containment building at power, the failure of an RCP such that missiles are generated and the pump casing is breached could result in a Loss of Coolant Accident (LOCA); LOCAs are considered in Chapter 9 of this PCSR. Any subsequent missile damage would be mitigated by the barriers provided by the in-containment Class 1, Seismic Category I structures.

133 Pumps, fans, motors and motor operated valves outside the containment building are designed, manufactured, operated and maintained such that the potential for generating missiles is significantly minimised. These components are segregated from Class 1 SSCs inside the containment building by the shield building and containment buildings which provide protection against missiles which are bounded by those considered in the assessment for wind generated missiles. The potential for damage to Class 1 SSCs outside of the containment building is precluded through the segregation of SSCs from equipment with the potential to generate missiles.

134 The potential consequences of the failure of rotating equipment located outside the containment building will depend on the location of the equipment in terms of the systems on which any failures occur. The failure of a pump in a primary circuit related system may result in a leak of primary circuit liquor into a compartment. In this case any missile generated would then be prevented from rendering Category A safety functions unavailable by the structural barriers provided.

3.2.5.2.3 Pressurised Components

135 Pressurised components include items such as pressure vessels, pump bowls, valves, pipes, pipe components and instrumentation that are part of systems that are operated or maintained at a maximum operating temperature greater than 93.3°C and/or a maximum operating pressure greater than 1.896 MPa. The worst case consequence for this type of failure is represented by the failure of primary circuit components. Any failure that could generate missiles may result in a LOCA. However, the description below argues that the structural barriers inside the containment building ensure that the potential consequences resulting from any missile impact are acceptable.

3.2.5.2.4 Explosions

136 Missiles can potentially be generated by explosions. The PCSR considers missiles generated from an explosion in the hydrogen storage area involving a full storage tank, gaseous hydrogen storage cylinders which supply hydrogen to the CVS and lorries delivering hydrogen to site.

137 The PCSR concludes that the consequences of missiles generated from a full hydrogen storage tank explosion or from the hydrogen storage cylinders on board delivery lorries will be bounded by those considered in the external hazards assessment of wind generated missiles.

138 The PCSR also concludes that generation of missiles due to an explosion caused by hydrogen released from the supply line to CVS is very unlikely. The PCSR judges that even if the single cylinder becomes a missile, the size and energy will be bounded by the wind generated missiles.

3.2.5.2.5 Falling Objects and Secondary Missiles

139 Outside of the containment building falling objects heavy enough to generate a secondary missile are postulated as a result of movement of a heavy load or from a non-seismically designed structure, system, or component during a seismic event. Movements of heavy loads are controlled to protect Class 1 SSCs.

140 Inside the containment building falling objects heavy enough to generate a secondary missile are postulated as a result of movement of a heavy load or from a non-seismically

designed structure, system, or component during a seismic event. Movements of heavy loads are controlled to protect Class 1 SSCs. Design and operational procedures of the polar crane inside containment precludes dropping a heavy load. Additionally, movements of heavy loads inside containment occur during shutdown periods when most of the high-energy systems are depressurised.

3.2.5.2.6 Redundancy, Separation and Segregation

141 The location and level of redundancy of Class 1 and 2 safety systems within the plant is such that complete loss of operability of the SSCs within a room or compartment from an internally generated missile would not result in loss of the Category A safety function.

142 Adequate redundancy is provided within each Class 1 safety system such that even if the loss of a single SSC were to occur the Category A safety function can still be provided by a redundant train located in a different compartment of the containment building or separated by sufficient distance. This compartmentalisation of Class 1 and Class 2 safety systems provides protection from system disruption due to any internally generated missile impact.

3.2.5.2.7 Further Mitigation

143 The plant is designed such that it can be operated with sufficient levels of protection in place to ensure that internally generated missiles will not prevent delivery of Category A safety functions. This defence in depth is provided by:

- The conservative design of equipment, the manufacture, maintenance and operation of that equipment in accordance with safety margins (through compliance with recognised design codes) appropriate engineering practices and monitoring of the quality of these aspects.
- Use of structural barriers to limit the path of any missile generated to areas where damage will not prevent the delivery of Category A safety functions.
- Sufficient redundancy and defence in depth is provided to ensure that even if there is the loss of any SSC as a result of an internally generated missile the Category A safety function can still be delivered.

3.2.5.2.8 Conclusions

144 The PCSR concludes that the likelihood of loss of Class 1 and 2 SSCs as a result of an internally generated missile is extremely small and has been addressed in the design of the plant and by normal operational procedures. Thus, the risks posed from internally generated missiles are at such a low level that measures to reduce the risk further are not considered to be practicable.

3.2.6 Release of Toxic, Corrosive or Flammable Material

145 The PCSR addresses the hazards arising from toxic, corrosive or flammable materials that may be required to be stored on site. The precise selection of chemicals and volumes may change based on site-specific requirements and operating experience and therefore storage and use of chemicals not identified in this chapter or present in

significantly greater concentrations or volumes will need to be justified on a site-by-site basis.

146 Potentially hazardous non-nuclear materials could threaten nuclear safety in the following ways should it accidentally be released:

- By causing a fire.
- By causing an explosion.
- By asphyxiating or poisoning personnel when those personnel are required to respond to a challenge to nuclear safety.
- By causing operating diesel engines to fail to start or shut down, if their function is required to support nuclear safety.
- By chemical or corrosive attack on SSCs.
- By causing brittle fracture of structural SSCs.
- By causing a criticality excursion, should the material be a moderator and it spills onto nuclear material.

147 The PCSR assumes certain material and volumes stored on site and states that the precise selection of chemicals and volumes stored on site may change based on site-specific requirements.

The PCSR considers the type, quantities and locations of hazardous material stored and, for each material in turn, the potential consequences of an uncontrolled release is described and the lines of defence identified.

3.2.6.1 Safety Design Approach Against Release of Toxic, Corrosive or Flammable Material

148 The principal area of concern is the NI, as this is where the Class 1 and most of the Class 2 SSCs are located, and where the majority of safety-significant required actions take place.

149 The risk from a release of toxic, corrosive and flammable materials is minimised by ensuring:

- Bulk storage of gases and chemicals is in locations where an uncontrolled release cannot threaten Class 1 SSCs.
- Storage of gases and chemicals are in vessels and containers that are constructed to appropriate codes of practice and where necessary provided with secondary containment (e.g. bunds or dykes) to contain accidental spills and leaks.
- Transport of material from the bulk storage location to local storage or use locations will be carried out in accordance with procedures and by processes that minimise the risk of an uncontrolled release of material.
- Materials are held and used in the minimum quantities within the NI necessary for AP1000 operation.
- Other intrinsically hazardous materials are present on site, but in such small quantities as to pose minimal threat and will be risk assessed and controlled by procedures and permits-to-work.

3.2.6.2 Redundancy, Separation and Segregation

150 The containment structure provides a barrier to the intrusion of toxic gases into the area where the main components of the Class 1 SSCs are sited. Outside the containment structure, the plant and its Class 1 SSCs have been designed so that the complete loss of the equipment within any single room will not result in loss of the Category A safety function. The fire barriers protecting redundant trains of the Class 1 SSCs from fire should also provide an adequate barrier to spread of corrosive liquids and toxic or flammable gases and therefore limit any damage to the equipment in one room.

151 DGs rely on an air supply to maintain their function. The Diesel Generators (DGs) are located in the DG building which is remotely sited from the other plant buildings and is on the opposite side of the turbine building to the Plant Gas System (PGS). The DG building and motor air inlets are located close to the ground so that the heated gases from a postulated fire affecting a diesel oil storage tank will not prevent DG motor start or operation. In addition, the batteries providing power to the Class 1 SSCs would not be susceptible to an asphyxiant gas.

152 Adequate redundancy is provided within each Class 1 safety system such that even if the loss of a single SSC as a result of, for example a fire which is assumed to disable the whole train, the Category A safety function can still be provided by a redundant train located in a different fire compartment (or fire zone within the containment building). This compartmentalisation of safety systems also provides protection from system damage due to ingress of toxic or corrosive liquids. In addition, penetrations between compartments are minimised mainly to reduce the potential routes for the spread of gases.

153 Taking account of the potential loss of those SSCs affected by the toxic, corrosive or flammable material concurrent with a credible unrelated single failure within the other SSCs the PCSR concludes that sufficient redundancy, diversity and segregation is provided in the design and location of the SSCs ensuring that the Category A safety functions are maintained in the worst, normally permitted, plant line-up.

3.2.6.3 Further Mitigation

154 The PCSR states that further mitigation against toxic, corrosive or flammable materials is provided by a combination of the following:

- The distance between the area where bulk liquefied gases are stored and the NI.
- The distance between the area where the bulk diesel oil is stored and the DG building and the NI.
- All pressure vessels are constructed and tested to the appropriate American Society of Mechanical Engineers (ASME) codes of practice.
- Losses of bulk liquefied gases are alarmed to the Main Control Room (MCR).
- The storage arrangements for bulk chemicals are such that they do not represent a significant threat to any Class 1 or Class 2 SSCs and no actions required to maintain Category A safety functions take place in a location where potentially toxic, corrosive, or flammable materials are stored.

- Storage and use of chemicals on the site must, where the specific Tier 1 or Tier 2 criteria are met (e.g. hydrazine), comply with the COMAH Regulations 1999 which require the operator to take measures necessary to prevent major accidents and limit their consequences to persons and the environment.
- All chemicals stored and used on the site must comply with the COSHH Regulations which requires that all chemicals, products containing chemicals, fumes, dusts, vapours, mists and gases (including asphyxiating gases) that are deemed to be hazardous to health are suitably controlled.
- Storage and use of chemicals that are potentially toxic, corrosive or flammable within the NI or turbine building are maintained at the minimum volumes required for the tasks to be undertaken.
- All gases delivered into the containment or the turbine building are via small bore piping which prevents a sudden high volume release of gas occurring.
- The Containment has hydrogen monitors to detect a rise in hydrogen concentration and automatic shut off valve for the hydrogen feed pipe.
- All Class 1 SSCs have redundant trains separated into zones for the prevention of loss by any single localised event such toxic gas or corrosive liquids.

3.2.6.4 Conclusions

155 The PCSR concludes that the measures outlined above demonstrate that the risk of loss of a nuclear safety significant system as a result of loss of corrosive, toxic or flammable materials is extremely small and has been addressed in the design of the plant (or will be addressed on a site-by-site basis), and by normal operational procedures and maintenance activities. The risks posed from corrosive, toxic or flammable materials are at such a low level that no practical measures to reduce the risk further could be identified.

3.2.7 Dropped Loads and Load Mishandling

156 The PCSR considers loads dropped from the polar crane, cask handling crane, refuelling machine, fuel handling machine, the new fuel elevator and from the fuel transfer system. The PCSR does not consider loads dropped from other cranes and lifting equipment, because the design has not progressed to the detailed design stage.

157 Loads dropped by cranes and other types of lifting equipment could prevent the delivery of Category A safety functions either directly through the load impacting with an SSC, or indirectly because of the collapse of a floor or wall that causes failure of the SSC. Additionally, potential damage can be caused by the mishandling of a load e.g. due to load swinging, ledging or attempting to lift a load still attached to an SSC.

3.2.7.1 Safety Design Approach to Dropped Loads and Load Mishandling

158 The PCSR states that cranes and lifting equipment to be used within the NI have been identified, together with the SSCs delivering Category A safety functions that could be impacted by a dropped load from this equipment. For some crane lifts, it can be shown that a dropped load will not impact SSCs delivering Category A safety functions. Where

SSCs delivering Category A safety functions can be impacted it is shown for the majority of lifts that other SSCs will continue to provide the Category A safety functions.

159 The PCSR identifies a number of lifts for which a dropped load has the potential to cause loss of a Category A safety function. These are limited to those that either require the lifting of nuclear fuel or lifting of loads over nuclear fuel. These occur within containment during refuelling operations when the reactor head is being removed or has been removed and in the radiological auxiliary building for fuel movements. The risk due to a dropped load for these lifting operations has been reduced to levels which are As Low As Reasonably Practicable (ALARP) through application of best practice to the design and operation of the cranes, together with procedural controls. The cranes used for these operations will almost exclusively:

- Be single failure proof (5 of the 16 lifting devices).
- Be fail-safe on loss of motive power.
- Be fail-safe in the event of a design basis seismic event.
- Have crane controls that allow precise positioning of loads.
- Have monitoring and protection devices to mitigate the risk of a dropped load, overload or crane collapse.
- Have safe load paths specified.
- Have procedural controls linked to plant operating mode to reduce the consequences of a dropped load.
- Have physical stops to prevent the hook from travelling over or near SSCs.

160 The PCSR also identifies a number of cranes, such as the hoist for handling spent fuel on the fuel handling machine, that are not single failure proof but which have single failure proof features. These features reduce the frequency of a dropped load and are combined with lift height limitations to ensure that the risk is reduced to a level that is ALARP.

161 The consequences of dropped loads are minimised by ensuring that loads that have to be lifted above SSCs delivering Category A safety functions are moved by:

- At the minimum height compatible with safely completing the move.
- Have safe load paths specified.
- Have physical stops to prevent the hook from travelling over or near SSCs.
- Have procedural controls linked to plant operating mode to reduce the consequences of a dropped load.

162 Statements on operating limits and conditions of cranes and lifting equipment are available and will be developed by the Licensee to provide a complete statement of the operating limits and conditions for the cranes and lifting equipment.

163 Floors and walls that could be impacted by a dropped load are required to withstand the potential dropped load without loss of function or disruption to other SSCs, where failure could lead to the loss of a Category A safety function. If this is not possible then load paths have been specified to ensure that a dropped load over a Category A safety function will not occur. The substantiation of the floor and wall structures for dropped loads is still to be carried out.

3.2.7.2 Dropped Loads Hazard Analysis

164 The cranes and lifting equipment considered by the PCSR are:

- Cranes and lifting platforms within the NI.
- Cranes and lifting platforms not in the NI.
- Monorail hoists.
- Elevators (lifts).
- Other lifting equipment.

165 For each building the lifting equipment is reviewed to determine the threat that a dropped load could pose and the measures that have been taken to minimise this threat both in reducing the frequency of a dropped load and then ensuring that the consequences are ALARP.

3.2.7.3 Conclusions

166 The movement of loads within the AP1000 during, normal operation, maintenance and refuelling is required for the continued correct functioning of the AP1000. While these operations have to be performed the risk has been reduced to a level that is ALARP by:

- Only carrying out lifting operations within the containment when the reactor is shutdown and in plant mode 5 (cold shutdown, when no Class 2 SSCs can be impacted by a load drop) or in plant mode 6 (refuelling).
- Minimising the frequency of a dropped load by using a single failure proof crane or one having single failure proof features where there is the possibility of disruption Category A safety functions with a dropped load.
- Minimising the consequences of a dropped load by minimising the lift height of a load.
- Providing crane instrumentation and control systems that act to prevent the crane structure and load bearing SSCs from being operated outside their design intent.
- Construction of AP1000 floor and wall structures to withstand the maximum dropped load for loads lifted above them without loss of function or disruption to Category A safety functions.

167 In addition to the engineered protection features described in this section, to reduce the risk from a dropped load, it is recognised that the operational control of lifting activities is also of importance. The control and operation of lifting equipment on the AP1000 will be carried out in accordance with the Licensee's written processes and procedures and statutory legislation and guidance.

168 Operational controls will also be applied by the Licensee to ensure that the number of lifts are minimised and that safe load paths are defined to minimise the potential for disruption to other SSCs.

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR INTERNAL HAZARDS

169 The Step 3 assessment report (Ref. 17) focused on Revision 1 of the PCSR (Ref. 18) and Revision 0 of the European Design Control Document (EDCD) (Ref. 19) for the AP1000. The AP1000 Step 3 Internal Hazards Assessment concluded that the PCSR and the EDCD were presented in a structure that was not in line with my expectations relating to the requirement for Westinghouse to present a claims, arguments and evidence

approach to the safety case. A Regulatory Observation (RO-AP1000-031) (Ref. 21) was raised during Step 3 with the need to provide an adequate safety case for internal hazards. The associated Regulatory Observation Action (RO-AP1000-031.A1) required Westinghouse to demonstrate that all claims made on SSCs in place to prevent an internal hazard occurring and/or prevent escalation of an internal hazard be identified and the appropriate arguments and evidence provided to demonstrate that the protection against such hazards has been adequately substantiated.

170 The means by which Westinghouse proposed addressing the RO was by providing an Internal Hazards Topic Report which included the claims, arguments and evidence for the internal hazards aspects of the AP1000 design. The Internal Hazards Topic Report was not assessed at Step 3 due to insufficient time for a detailed assessment and as a result has been subject to assessment during Step 4.

171 Following on from the production of the Internal Hazards Topic Report, Revision A of the PCSR (Ref. 1) was issued. It is accepted that Revision A of the PCSR is currently in draft, however, it is contained within the Master Submission List and in order to verify the statements made therein, a series of targeted confirmatory TQs (Ref. 21) were raised to capture changes from Revision A that are to be contained within the final issue of the PCSR. As a result Revision A of the PCSR coupled with information contained within the Internal Hazards Topic Report has been used as the basis of this assessment report.

172 Section 11.1 of the PCSR (Ref. 1) states that "*the internal hazards assessment is documented in the internal hazards topic report [Ref. 11.3] from which this PCSR chapter is derived*." As a result Revision 2 of the Internal Hazards Topic Report has been identified as a key submission which the PCSR is reliant on to provide the claims, arguments and evidence associated with internal hazards. In addition, the PCSR makes extensive reference to the AP1000 Barrier Matrix (Ref. 22) for further details on the location and design qualification of the hazard barriers and their penetrations.

173 The Step 4 assessment builds on the assessment undertaken at Step 3 and is focused on the claims, arguments and evidence presented in the PCSR and its supporting documents; Internal Hazards Topic Report and AP1000 Barrier Matrix.

174 As part of the assessment undertaken during Step 4, two separate pieces of work were undertaken by TSCs associated with internal hazards. Atkins undertook an assessment of internal fire, explosion and missile, while Frazer Nash undertook assessment which included pressure part failure, dropped loads and impact, and internal flooding. The assessment undertaken was based upon Revision 1 of the Internal Hazards Topic Report (Ref. 15) issued to ND in February 2010. It is recognised that this version of the topic report was revised in September 2010, however, the information contained within the assessment undertaken by both TSCs was provided to Westinghouse to inform the future revision. I have included some of the main conclusions from the assessments undertaken specifically within the Sections 4.1 and 4.2 of this report, however, I have also included specific conclusions within the relevant sections of the assessment report relating to fire, flood, pressure part failure, explosion, missile, and dropped loads and impact, where applicable. As the assessments are based upon Revision 1 of the Internal Hazards Topic Report, I believed it made this assessment report clearer if I included the conclusions of the TSC assessment at the start of my assessment report, as my detailed assessment is based upon the PCSR that should have addressed all the concerns arising from the TSC assessment that was undertaken.

175 With the exception of the two sections that detail the outcome of the early assessment work undertaken by TSCs, the structure of this assessment is through assessment by

hazard area. This aids in the structural presentation and the clarity of the assessment report. A comparison of standards, guidance and relevant good practice is included on a hazard by hazard basis, as are overall conclusions for each internal hazard. There are conclusions drawn within each of the specific areas of assessment that present my judgement on the adequacy of the AP1000 design for the areas sampled as well as reference to the associated GDA Issues or Assessment Findings raised as part of my assessment.

176 It is important to stress that the two pieces of TSC assessment undertaken were on an earlier revision of the PCSR and Internal Hazards Topic Report. Westinghouse have since addressed a number of the conclusions raised within the TSC assessments and, as a result, the conclusions drawn from the assessments undertaken may not all be current, however, it is important that the salient points of the assessments undertaken are captured within my Step 4 Assessment.

4.1 Atkins Assessment of the Westinghouse AP1000 in Relation to Internal Fire, Explosions and Missiles

177 During Step 4 Atkins were employed to provide an independent assessment of Revision 1 of the Internal Hazards Topic Report which had been supplied to ND early within Step 4. My objective for the independent assessment was to confirm that my initial assessment of the Internal Hazards Topic Report was consistent with the expectations of other recognised technical specialists within the internal hazards discipline. The following objectives were, therefore, set out:

- Atkins to undertake an independent assessment of the Westinghouse AP1000 Internal Hazards Topic Report, Revision 1, specifically addressing internal fire, explosion and missiles on a sampling basis and to examine the submission based upon the claims, arguments and evidence approach as detailed within ND guidance AST/001.
- The SAPs, international relevant good practice and standards as well as operational experience both within the UK and overseas will be used to inform the assessment undertaken.
- The approach to the assessment undertaken by Atkins was to adhere to a clear claims, arguments, and evidence approach in the format and structure of the reporting.

178 It is important to recognise that the Atkins report (Ref. 23) was issued in June 2010 and following its my acceptance of the report a copy was provided to Westinghouse in order to inform them of the outcome of the review and to allow them to address the comments made therein. It is recognised that the assessment produced by Atkins was undertaken on documentation that has since been superseded; however, it is important to include the findings within this assessment report given the applicability of the comments made.

179 An overview of the assessment undertaken by Atkins is included within this section of my assessment report.

4.1.1 Scope of Assessment Carried Out

180 The assessment undertaken by Atkins involved a high level review of Revision 1 of the Internal Hazards Topic Report which included consideration of the key references, namely, Revision A of the AP1000 Barrier Matrix (Ref. 22), Revision 0 of the AP1000

Safety Categorisation and Classification Methodology (Ref. 25), Revision 0 of the AP1000 Safety Categorisation and Classification of Structures, Systems and Components, and Revision 1 of the European Design Control Document (EDCD) (Ref. 26).

181 The assessment also took into account the findings raised by ND during Steps 2 and 3 with a view to establish whether they had been adequately addressed within Revision 1 of the Internal Hazards Topic Report.

4.1.2 Summary of Assessment

182 The following provides an overview of the key aspects of the Atkins assessment undertaken:

- The assessment identifies that the EDCD does not provide adequate substantiation for the fire resistance claims being made on the fire barriers. The report states, *"Reference 12 [EDCD] also states that the barriers (including dampers, walls, doors, cable tray enclosures, seals etc.) are rated against the most onerous fires. Based upon the evidence provided, this statement is not substantiated."*
- Again, the reference to the AP1000 Barrier Matrix for substantiation does not provide sufficient evidence by which the adequacy of the fire barrier can be demonstrated. The report states, *"Reference 2 [AP1000 Barrier Matrix] does not provide the appropriate evidence to justify the selection of equipment (i.e. fire barriers) required to fulfil their safety function."*
- The assessment identified that the claims associated with the qualification of barriers in place to withstand the pressure loads caused by an internal explosion have not been supported with adequate arguments and evidence.
- Also within the area of internal explosion, the Internal Hazards Topic Report claims that the hydrogen supply within Containment is limited to the contents of a single bottle and would not result in an explosion if the entire contents were released. The assessment considered that further justification is required as the over-arching claim is not supported by detailed arguments and evidence associated with the postulated release location, size of the compartment, potential ignition sources, and the degree of confinement.
- The potential for an explosion within the battery rooms was also subject to assessment by Atkins, who stated, *"Section 9.5.13 of Reference 1 [Internal Hazards Topic Report Revision 1] states that the Battery Rooms outside containment are ventilated by a system that is designed to preclude the possibility of hydrogen accumulation. Thus, the report considers that such an explosion within the Battery Rooms as a beyond design basis event, as it requires triple failure of the ventilation system and failure of the monitoring of the ventilation system. An engineering judgement was made that a hydrogen explosion from the Battery Rooms would not propagate to other Battery Rooms and affect nuclear safety. This statement makes an implicit claim on the role that the ventilation system plays in preventing an explosion. Furthermore, the design basis assessment should initially assess the unmitigated consequences, therefore, this fault is not a beyond design basis event."*
- With regard to the analysis of internal missiles, the assessment stated, *"Section 10.1.1 of Reference 1 [Internal Hazards Topic Report, Revision 1] reports the approach taken to deal with internal missiles including minimisation of potential*

sources in the safety related buildings, appropriate design, construction, operation and maintenance of components that could potentially generate missiles, barrier qualification to withstand the effects of internal missiles on the area, and qualification of nuclear safety related plant, where appropriate. However, the report failed to provide sufficient argument and evidence to support the above."

- Furthermore, the assessment identifies that there are a number of claims made associated with missile barriers, however, the claims are qualitative in nature and there is no withstand justification or qualification provided.

4.1.3 Conclusions

183 The findings of the Atkins assessment were used to further inform my assessment during Step 4. As mentioned previously the Atkins assessment has been provided to Westinghouse and areas were identified as requiring further supporting substantiation during Step 4.

4.2 Frazer Nash Assessment of the Westinghouse AP1000 in Relation to Pressure Part Failure, Dropped Loads and Impact, and Internal Flooding

184 During Step 4 Frazer Nash Consultancy were employed to provide an independent assessment of Revision 1 of the Internal Hazards Topic Report which had been supplied to ND early within Step 4. As was the case for the assessment work undertaken by Atkins, the objectives of the independent assessment were to confirm that my initial assessment of the Internal Hazards Topic Report was not unduly onerous or inconsistent with the expectations of other recognised technical specialists within the internal hazards discipline. The following objectives were, therefore, set out:

- Frazer Nash Consultancy to undertake an independent assessment of the Westinghouse AP1000 Internal Hazards Topic Report, Revision 1, specifically addressing internal flooding, pressure part failure, internal missile and dropped loads and impact, on a sampling basis and examine the submission based upon the claims, arguments and evidence approach as detailed within ND guidance AST/001.
- The SAPs, international relevant good practice and standards as well as operational experience both within the UK and overseas will be used to inform the assessment undertaken.
- The approach to the assessment undertaken by Frazer Nash Consultancy was to adhere to a clear claims, arguments, and evidence approach in the format and structure of the reporting.

185 Again, as the case for the Atkins assessment, it is important to recognise that the Frazer Nash Consultancy (Ref. 27) report was issued in May 2010 and following its acceptance by me a copy was provided to Westinghouse in order to inform them of the outcome of the review and to allow them to address the comments made therein. It is recognised that the assessment produced by Frazer Nash Consultancy was undertaken on documentation that has since been superseded; however, it is important to include the findings within this assessment report given the applicability of the comments made.

186 An overview of the assessment undertaken by Frazer Nash Consultancy is included within this section of my assessment report.

4.2.1 Scope of Assessment Carried Out

187 The assessment undertaken by Frazer Nash Consultancy involved a high level review of Revision 1 of the Internal Hazards Topic Report which included consideration of Revision A of the AP1000 Barrier Matrix and Revision 1 of the EDCD.

4.2.2 Summary of Assessment

188 The following provides an overview of the key aspects of the Frazer Nash assessment undertaken:

- The assessment states that the main safety claims within the Internal Hazards Topic Report associated with internal flooding events either do not affect safety related SSCs or that they are adequately protected against their effects. The report cites that this approach seemed reasonable, however, the claims do not appear to be worded as claims given their high level qualitative nature.
- The assessment states that a comprehensive flood analysis has been carried out and that Internal Hazards Topic Report does make claims on the leak tightness of doors; however, it does states that there is a ½ inch gap beneath the doors to which the assessment points out that this is in fact a claim on the doors to perform this function.
- The assessment also questions whether the flood hazard analysis undertaken considers blockage of drains, or malfunction of back flow preventers that might inhibit water flow.
- The assessment states that a crucial argument is associated with break exclusion zones near to penetrations through the containment associated with main steam and feed pipework. The assessment states, *"This is effectively an Incredibility of Failure (IoF) claim. The UK SAPs contain special provisions for IoF claims, but these do not appear to have been addressed in the referenced Section 3.6.2.1.1.4. of the EDCD."* . [It should be noted that the SAPs do not actually make reference to the term Incredibility of Failure (IoF) but that Principles EMC.1 to EMC.3 are applied to the highest integrity components which are often referred to as being IoF.]
- In relation to internal missile, the assessment states, *"There are various sub-claims stated in the topic report that don't add a great deal and are confused somewhat with arguments."*
- In addition, the assessment identifies that the arguments presented associated with separation, orientation and barriers, and questions the potential for missiles affecting containment from sources either within the Containment Building or within the Turbine Building.
- The assessment identifies that the main claims made in the area of dropped loads and impact are that they are precluded by design, to the extent practicable, and that where this cannot be achieved, complete loss of operability of equipment in an area experiencing a dropped load would not compromise delivery of the Key Safety Functions. The assessment points out that there is uncertainty associated with the phrase *"to the extent practicable"* regarding what is actually meant and whether this has involved an ALARP assessment associated with dropped loads and impact.
- Once again within the area of dropped loads and impact, the assessment identifies that, *"There are various sub-claims stated in the topic report that don't add a great deal and are confused somewhat with arguments."*

- The assessment identifies that there are safe lifting paths designated for “heavy load” lifts, however it identifies that the Internal Hazards Topic Report is not clear and seems rather arbitrary. The assessment questions how such load paths would be enforced, by administrative controls alone or by the use of engineered protection systems. In addition, it is not clear whether load drops from smaller lifts is insignificant and this does not appear to have been considered within the Internal Hazards Topic Report.
- In each of the areas assessed by Frazer Nash Consultancy they identify that, *“very little evidence is presented in the topic report to support the arguments”*.

4.2.3 Conclusions

189 The findings of the Frazer Nash Consultancy assessment were used to further inform my assessment during Step 4. As mentioned previously the Frazer Nash Consultancy assessment has been provided to Westinghouse and areas were identified as requiring further supporting substantiation during Step 4.

4.3 Nuclear Directorate Assessment of Internal Fire

190 The AP1000 Step 3 Internal Hazards Assessment and AP1000 Step 4 Assessment Plan identified the need for further assessment of the following internal fire related aspects associated with internal hazards for during Step 4:

- AP1000 Fire Hazards Analysis
- Fire Resistance Claims Associated with Nuclear Significant Hazard Barriers
- Nuclear Significant Hazard Barrier Penetrations
- Cable Segregation and Separation
- Exceptions to Segregation
- Spurious Operation and Common Cause Failure
- Fire Protection System

4.3.1 AP1000 Fire Hazards Analysis

191 As stated earlier in Section 4, the Step 3 Assessment did not assess the Internal Hazards Topic Report and as a result is part of the assessment undertaken by ND during Step 4. Appendix A of the Topic Report details the outcome of a room by room fire analysis which has been subject to assessment within this section of my assessment report.

4.3.1.1 Scope of Assessment Carried Out

192 My assessment focused on a sample of rooms within the fire hazard analysis and considered the approach taken to the analysis as well as the detailed claims, arguments and evidence presented therein.

4.3.1.2 Assessment

193 Section 4.1 of the Internal Hazards Topic Report states:

"*In considering the safety arguments for internal fire hazards the requirement is to show that any postulated internal fires within the design basis do not prevent the delivery of the Category A safety functions and the supporting Category B safety functions. The overall approach is to:*

- *Assess the consequences should an ignition source be present (whether one is likely to be present or not) i.e. deterministically assume that a fire is initiated.*
- *Ensure combustible loads are reduced so far as is reasonably practicable.*
- *Demonstrate that:*
  - *the SSCs are qualified to withstand the internal fire hazard.*

or

  - *that there are sufficient redundant trains of SSCs providing the nuclear safety functions and that the trains are segregated from each other such that and any credible internal fire will not prevent delivery of the Category A or the Category B supporting functions.*

or

  - *SSCs are segregated from areas containing significant fire hazards.*

This fire hazard analysis considers the provision of fire control in AP1000 plant areas, with particular focus on those areas containing Class 1 SSCs i.e. the NI (the shield/containment building and the auxiliary building)."

194 The approach taken to the production of a fire hazard analysis is in line with both internal and external standards and guidance, most notably, TAG, T/AST/014, and IAEA guidance, NS-G-1.7. The structure of the fire hazards analysis is clear and identifies any potential threats to safety significant SSCs and identifies individual fire zones, fire loads, segregation and separation provisions as well as the effects on redundant plant and equipment.

195 The following fire area and zone analyses contained within the fire hazard analysis were sampled as part of my assessment:

- Fire Area 1240 AF 01 – Non-Class 1E equipment/penetration room.
- Fire Area 1202 AF 04 – Division A battery room, DC equipment room and C&I room.
- Fire Zone 1100 AF 11301 – Steam Generator compartment 1
- Fire Zone 1100 AF 11500 – Operating Deck and Refuelling Cavity

196 The four areas sampled were selected as two are contained within the Auxiliary Building where there is the provision of fire barriers to ensure fire does not spread beyond the fire area and two are within the Containment which relies more on localised protection and geographical arguments.

4.3.1.2.1 Fire Area 1240 AF 01 – Non-Class 1E Equipment/Penetration Room

197 The analysis states that the potential fire loading is approximately 510MJ/m^2 which equates to an approximate fire resistance time of 34 minutes and the room is within a 3 hour fire compartment. Class 1 cables associated with Division A and C are routed through the room and as a result there is the potential for the equipment being fed by cables routed through this room to be lost, specifically:

- Control of the Division A Containment Isolation Valves is outside Containment, however, in this event there are redundant isolation valves within Containment that are powered and controlled from outside this compartment.
- Control of Division A and C Passive Containment Cooling System isolation valves, however the redundant Division B isolation valves would be unaffected by a fire within this compartment and as a result the Category A functionality of the passive containment cooling system is maintained.

198 The potential for spurious actuation/operation of the squib valves off the Diverse Actuation System (DAS) is also considered, however, this aspect of the assessment is considered within the Section 4.3.6 of this assessment report.

199 The consideration of total room burnout and loss of all equipment contained therein is in line with my expectations. The fire loading within the room is within the 3 hour withstand of the claimed barriers and the room is protected by fire dampers to ensure that fire cannot spread beyond the room of fire origin. The assessment of fire dampers is included within Section 4.3.3 of this assessment report.

200 I am satisfied that the fire hazard analysis has adequately addressed fire within this fire area and the conservatism applied to loss of all equipment within this area is in line with my expectations.

4.3.1.2.2 Fire Area 1202 AF 04 – Division A Battery Room, DC Equipment Room and C&I Room

201 This fire area contains Class 1 equipment associated with the Class 1E DC and Uninterruptible Power Supply including the batteries, DC and DC distribution panels, the AC inverter, transformer, battery chargers, and protection and monitoring system cabinets.

202 The highest fire load is within the DC equipment room and has been calculated to be approximately 770MJ/m^2 which equates to a fire loading of approximately 50 minutes and all three rooms are contained within a single 3 hour fire compartment. The rooms are horizontally segregated with one hour fire barriers which would prevent propagation vertically and as a result the calculated fire loadings should limit the spread of fire to the individual rooms, albeit, the ductwork is not provided with fire dampers, however, it is assumed that a fire within this compartment would result in loss of all function contained within all three rooms.

203 The doors to the rooms are fed from a common corridor and should the door to the room in which the fire is located be open, there would be a need for a further door within another 3 hour fire barrier to be open to result in loss of more than one Division. TQ-AP1000-1280 was raised seeking confirmation that there are door control procedures associated with doors within nuclear significant hazard barriers. The response provided details of the alarms, annunciation, and included reference to a detailed functional specification (Ref. 28) for the systems to be installed on the different types of doors included within the AP1000 design. The reference was subject to a limited review and found to be in line with my expectations for ensuring that doors within nuclear significant hazard barriers are monitored and alarmed. The functional specification provides detailed technical information relating to the design and installation of the door monitoring systems.

204 I am satisfied that the fire hazard analysis has adequately addressed fire within this fire area and the conservatism applied to loss of all equipment within this area is in line with my expectations. In addition, the provisions of door control procedures associated with the AP1000 design appears to be in line with my expectations.

4.3.1.2.3 Fire Zone 1100 AF 11301 – Steam Generator Compartment 1

205 This fire zone contains cabling associated with the two reactor coolant pumps and components contained within this fire zone. The fire load within the fire zone has been calculated as 72MJ/m^2 which equates to a fire resistance time of approximately 5 minutes. The fire loading is primarily associated with cabling and the fire hazard analysis states that the location of barriers assures that fire cannot spread from beyond this area.

206 The fire hazard analysis states that should there be a fire within this zone that it would be limited in size and the products of combustion, namely the smoke and hot gases, would quickly be cooled through air entrainment and contact with the structural surfaces of the barriers. The fire threat to the adjacent fire zones would not be susceptible to damage from a fire within this fire zone.

207 The approach taken to the components within this fire zone is to conservatively assume total loss of functionality, however, this is not anticipated given the low fire loading and the spatial separation of the cables contained within the fire zone. The safe shutdown components assumed to be lost within this fire zone are:

- All four Divisions of the reactor coolant system / reactor coolant pump bearing temperature instrumentation. As a result of this, there would be failure to detect and hence to provide a trip signal on loss of component cooling water to the pump. If the fire does not disable the pump, then the component cooling water flow to the pump would not be affected and it would continue to provide cooling water to the pump bearings. Should the pump be lost, then the remaining unaffected Reactor Coolant Pump (RCP) would be sufficient to ensure safe shutdown capability as it is located within a separate fire zone which would not be susceptible to loss due to a fire within this fire zone.
- The RCP shaft speed instrumentation, however, the redundant reactor coolant system hot leg flow instrumentation contained within fire zones 11300A and 11300B would be able to perform this function and would not be affected by a fire within fire zone 11301.
- The four reactor coolant system head vent valves, however, these are normally in the closed position and only required to operate in a fault condition. The potential for fire induced spurious operation is addressed within Section 11.4.6.2 of the PCSR relating to spurious actuation and has been considered as part of my assessment within Section 4.3.6 of this assessment report.

208 I am satisfied that the fire hazard analysis has adequately addressed fire within this fire zone and the conservatism applied to loss of all equipment within the fire zone is in line with my expectations.

4.3.1.2.4 Fire Zone 1100 AF 11500 – Operating Deck and Refuelling Cavity

209 The rooms included within the fire hazard analysis undertaken within this fire zone are:

- Operating deck.

- Refuelling cavity.
- Division B / D penetration room.

210 This fire zone contains cabling associated with Division B / D 1E electrical systems, core exit temperature monitoring, and steam generator narrow range level monitoring. The fire load within the fire zone has been calculated as 140MJ/m^2 which equates to a fire resistance time of approximately 9 minutes. The fire loading is primarily associated with cabling with small concentrations within horizontal cable trays located at high level around the circumference of the fire zone and vertical cable trays at separate locations adjacent to the boundary of the fire zone as well as in the vicinity of the reactor vessel integrated head package. The fire hazard analysis again states that the location of barriers assures that fire cannot spread from beyond this area.

211 As was the case for the previous fire zone assessed (1100 AF 11301), the fire hazard analysis states that should there be a fire within this zone that it would be limited in size and the products of combustion, namely the smoke and hot gases, would quickly be cooled through air entrainment and through contact structural surfaces. The fire zone encompasses most of the containment and walls of this fire zone comprise of the steel containment vessels or structural concrete. The fire hazard analysis states that the fire threat to the adjacent fire zones would not be susceptible to damage from a fire within this fire zone.

212 The fire hazard analysis again conservatively assumes loss of the safe shutdown components within this fire zone, namely:

- Division B and D electrical components, however, the Division A and C electrical components located within a different fire zone (1100 AF 11300B) are sufficient to ensure safe shutdown.
- In-core instrumentation system core exit temperature instrument termination cabinets, however, the wide range reactor coolant system hot leg temperature instrumentation located within fire zones 1100 AF 11301 and 1100 AF 11302 provide a diverse means by which to monitor the temperature of the reactor coolant.
- Reactor coolant system narrow range level instrumentation, however, there is the provision of redundant level instrumentation within fire zone 1100 AF 11300B which is sufficient to perform the requisite functions to achieve and maintain safe shutdown.

213 I am satisfied that the fire hazard analysis has adequately addressed fire within this fire zone and the conservatism applied to loss of all equipment within the fire zone is in line with my expectations.

4.3.1.3 Conclusions

214 From my sample of the above four rooms and areas, I am satisfied that a detailed fire hazard analysis has been undertaken that focuses on the potential fire threat to safe shutdown components within the AP1000 design.

4.3.2 Fire Resistance Claims Associated with Nuclear Significant Hazard Barriers

215 The hazard barriers are claimed in order to prevent loss of more than one redundant train of protection due to a range of internal hazards and forms the basis for the claims made for segregation within the AP1000 design. This aspect of my assessment has focused on

the claims made on such barriers in relation to their resistance to fire in terms of insulation, integrity and load bearing requirements.

4.3.2.1 Scope of Assessment Carried Out

216 The scope of the assessment undertaken during Step 4 was to consider the arguments and evidence associated with the fire resistance claims made relating to the nuclear significant hazard barriers.

217 The intent of the assessment was to sample the PCSR in order to identify the basis of the claims made through consideration of the arguments presented and through undertaking a deep slice sample into the evidence provided.

4.3.2.2 Assessment

218 The PCSR states that "*to prevent the spread of fires, passive fire protection measures such as fire resistant barriers and physical or spatial separation are used in the fire protection design of AP1000. Fire compartmentalisation is used extensively throughout AP1000. The AP1000 fire barriers are designed in accordance with BSI guidance and IAEA and their location and fire resistance is identified in the AP1000 Barrier Matrix*."

219 This claim was initially assessed through the consideration of the location and identification of the barriers identified within the AP1000 Barrier Matrix.

220 The AP1000 Barrier Matrix is the key source of evidence associated with the fire resistance of the barriers referenced within the PCSR. In addition, and as stated previously, the Internal Hazards Topic Report also provides detailed claims made on the barriers in relation to fire and has also been considered within the assessment.

221 For the Auxiliary and Containment Building the AP1000 Barrier Matrix identifies the barriers including the type of penetrations and the claimed fire resistance duration for the fire barrier. The HBM does not provide details of the substantiation of the claimed fire resistance; the PCSR cites that the provisions for the fire barrier construction are in accordance with *"relevant, applicable and appropriate guidance provided by international and US bodies, and British Standards (BS) and European Standards. For examples of these guidelines and standards, see References 11.8, 11.9, 11.10, 11.11, and 11.12."*

222 As part of the assessment, the references cited were checked to determine their applicability of the claim made relating to the materials of construction of the fire barriers. Reference 11.12 of the PCSR is a British Standard, BS EN 13501-1:2002, *"Fire classification of construction products and building elements. Classification using test data from reaction to fire tests."* (Ref. 29), which details the test criteria associated with the reaction to fire of construction products. This standard provides guidance relating to the contribution to fire provided by different elements of construction, namely whether or not they will burn, and does not consider the fire resistance requirements and the structure per se. Therefore, this standard does not provide the evidence and substantiation for the barriers in relation to fire resistance.

223 As a result the other references were subject to assessment to ascertain their validity in relation to the claims made within the PCSR. The other references cited are:

- IAEA NS-R-1, "Safety of Nuclear Power Plants: Design," (Ref. 11);
- NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," (Ref. 30)

- "The Building Regulations 2000, Fire Safety: Approved Document B. (Ref. 31);
- BS 9999:2008, "Code of practice for fire safety in the design, management and use of buildings," (Ref. 32).

224 In addition, the above references do not provide evidence to support the claims made upon the 3 hour barriers, they simply provide either guidance or stipulate that barriers should be provided. It is accepted that the barriers included within the design of the AP1000 should be capable of providing a 3 hour fire resistance based upon the inherent nature of their construction, however, there is no substantiation that such structures would be capable of doing so nor is there any reference to BS EN 1363, "Fire resistance tests" (Ref. 33), a European Standard associated with the ability of a fire barrier to withstand fire in terms of integrity, insulation and load bearing capacity as part of the substantiation. Given that adequate arguments and evidence have not been presented within the PCSR, a GDA Issue (**GI-AP1000-IH-01**) (see Annex 2) has been raised relating to the substantiation of the internal fire safety case, which includes an action associated with the substantiation of the 3 hour fire resistant barriers (**GI-AP1000-IH-01.A1**).

225 It is important to recognise that, although the most appropriate standards have not been explicitly referred to, the principle of four train segregation appears to be robust, with the identification of nuclear significant hazard barriers at the interface of each of separation train.

226 The approach to generating vertical fire resistant compartments is in line with my expectations for ensuring adequate segregation of trains of protection. The horizontal segregation within trains has not been substantiated within the PCSR including the use of notional one hour barriers without installed fire dampers. I would have expected to see such aspects of the design included within the substantiation given that the approach identifies the one hour barriers within the AP1000 layouts yet makes no comment over the design and provisions in place to minimise the potential for fire spread without necessarily providing the full protection that would have been anticipated for a one hour fire barrier. The aspects of cable routing and exceptions to segregation are considered within Sections 4.3.4 and 4.3.5 of this assessment report.

227 The PCSR does identify that there is a need for further substantiation of load bearing elements and states within 11.4.3.1, *"Structural elements protecting Class 1 SSCs provide 3 hour fire resistance for load bearing integrity. The substantiation for this fire resistance is to be addressed as part of the evidentiary process completion."*

4.3.2.2.1 Nuclear Significant Hazard Barriers Comprising of Modular Construction

228 There are 3 hour fire barriers included within the AP1000 design that are of a modular construction and it was uncertain, given the steel-concrete-steel construction of the modules and the structural claims made upon the exposed steelwork, whether such structures would be capable of meeting a 3 hour fire resistance requirement in relation to integrity, insulation and load bearing capacity. During Step 4, a TQ (TQ-AP1000-0913) (Ref. 21) was raised requesting a complete listing of barriers (vertical and horizontal) installed as part of the CA modular construction of the AP1000 that are claimed against the effects of fire and detail the specific requirements in terms of fire resistance duration. In addition it requested to provide the following:

- The specific fire testing undertaken on the barrier in relation to the integrity, the insulation, and the structural performance of the proposed system; whether the tests were constrained or unconstrained;
- Whether the fire assessment is based on structural collapse or on serviceability limit states;
- The structural loads considered as acting during and subsequent to a fire;
- Whether the fire capability of CA modules has been determined based on the performance of an isolated module or as a structurally constrained component within a structure;
- The stress-strain characteristics of the materials at elevated temperature;
- How the performance of plant support embedments has been determined.

229 The full response to this TQ was due to be issued to ND by the 24 September 2010 to enable adequate assessment to be undertaken during Step 4, however, the full response was not received until the 21 January 2011, and as a result there was insufficient time for the response to be subject to adequate assessment during Step 4.

230 Given that adequate arguments and evidence have not been presented within the PCSR and that there has been insufficient time during Step 4 to assess the response to the above TQ, a GDA Issue (**GI-AP1000-IH-01**) (see Annex 2) has been raised relating to the substantiation of the internal fire safety case, which includes an action associated with the substantiation of the 3 hour fire resistant barriers (**GI-AP1000-IH-01.A1**).

4.3.2.3 Conclusions

231 It is accepted that the claims made on the 3 hour fire barriers, other than those as part of the modular construction, can be substantiated given industry experience and knowledge of the robust nature of the construction. Unfortunately, the PCSR does not provide the requisite links through to the appropriate evidence by which these barriers can be verified as providing the 3 hour fire resistance.

232 There are also gaps in the safety arguments made; I would have expected to see a coherent argument, involving the process by which the 3 hour fire resistance is demonstrated including:

- Reference to physical fire testing or detailed supporting analysis (backed by appropriately verified and validated fire models) of the barriers and cable tray enclosures claimed;
- Detailed arguments associated with the approach taken to the horizontal segregation across individual trains within the Auxiliary Building and the use of notional 1 hour barriers without installed fire dampers;
- Substantiation of partial height barriers and barriers with penetrations that are not to be sealed;
- The approach taken to minimise penetrations within the barriers;

233 The information provided within the PCSR provides a useful overview of the principle claims made, but does not provide arguments and evidence to demonstrate that the principal claims will be met.

234 I am not satisfied that the substantiation of the 3 hour fire barriers for integrity, insulation and load bearing capacity has been adequately addressed within the PCSR and therefore as part of a GDA Issue relating to the substantiation of internal fire safety case, an action associated with the substantiation of the barriers claimed to provide 3 hours fire resistance for integrity, insulation and load bearing capacity (where applicable) has been raised:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Civil Engineering		
GDA Issue Reference	**GI-AP1000-IH-01**	**GDA Issue Action Reference**	**GI-AP1000-IH-01.A1**
GDA Issue	Internal Fire Safety Case Substantiation		
GDA Issue Action	Provide substantiation of the nuclear significant hazard barriers claimed to provide the level of fire resistance stated within the PCSR for integrity, insulation and load bearing capacity (where applicable). This may include a multi-legged argument consisting of the following: • Reference to physical fire testing or detailed supporting analysis (backed by appropriately verified and validated fire models) of the barriers and cable tray enclosures claimed. • The approach taken to minimise penetrations within the barriers. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

235 The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.3.3 Nuclear Significant Hazard Barrier Penetrations

236 The Step 3 Internal Hazards Assessment for the AP1000 stated, "*There are some aspects of the fire protection design e.g. fire barriers and their associated doors, fire dampers and penetration seals, that ND would expect to be classed as 'Safety' due to their function to ensure that fire did not spread to affect more than one train of protection. Within the UK nuclear fleet such items are identified as being necessary to ensure nuclear safety and adequate measures are taken to ensure that these SSCs are designed, maintained and controlled to ensure they perform their required safety function*". During Step 4 this aspect of the AP1000 design was subject to further assessment with a view to identification of the arguments and evidence in support of the claims made within the PCSR.

4.3.3.1 Scope of Assessment Carried Out

237 The scope of the assessment undertaken during Step 4 was to consider the arguments and evidence associated with the claims made relating to nuclear significant hazard barrier penetrations, including the provision of active fire dampers installed within the heating, ventilation, and air conditioning (HVAC) systems.

238 The intent of the assessment was to sample the PCSR in order to identify the basis of the claims made through consideration of the arguments presented and through undertaking a deep slice sample into the evidence provided.

4.3.3.2 Assessment

239 The approach to the design for AP1000 is to minimise the number of penetrations within nuclear significant hazard barriers including ventilation ductwork, cables, and pipework. The PCSR states that all penetrations are fire stopped to the same fire resistance (integrity and insulation) as the barrier they penetrate. The claim is therefore upon the doors, dampers and penetration sealing systems for cables and other miscellaneous penetrations. All penetrations including their size, service e.g. electrical, HVAC, piping etc. and their associated fire resistance is recorded within the hazard barrier matrix. It is stated within the PCSR that the penetration sealing will comply with relevant standards and guidance for ensuring that the barrier integrity is not compromised and that the penetrations provide the same fire resistance as the barrier they penetrate. The standards quoted within the PCSR to demonstrate that the penetrations contained within the design of the AP1000 will meet the requisite fire resistance (3 hours integrity and insulation) are:

- BS 476-31.1:1983, *"Fire tests on building materials and structures. Methods for measuring smoke penetration through doorsets and shutter assemblies. Method of measurement under ambient temperature condition."* (Ref. 34).
- LPS 1056, Issue 3, *"Requirements and Tests for Fire Doors of at Least Two Hours Fire Resistance,"* (Ref. 35).
- ISO 10294-1, *"Fire Resistance Tests – Fire Dampers for Air Distribution Systems"* (Ref. 36).
- BS EN 1366-2:1999, *"Fire resistance tests for service installations. Part 2: Fire dampers"* (Ref. 37).

These standards address requirements for doors and dampers, however, once again the European Standard, BS EN 1363-1 is not mentioned and given that this standard forms the basis for fire testing for most applications including fire doors and penetrations, this is very surprising. In addition, there is no mention of ensuring that the penetration sealing meets with the requirements of BS EN 1366-3, "*Fire resistance tests for service installations. Part 3: Penetration seals"* (Ref. 38). Furthermore, the standard referred to for testing of fire doors is a Loss Prevention Standard and not the British or European Standard applicable, namely BS 476: Part 22, *"Fire test on building materials and structures"* (Ref. 39) or BS EN 1634-1 *"Fire resistance test for doors and shutter assemblies- Part 1: Fire doors and shutters"* (Ref. 40). It is accepted that the Loss Prevention Standard references the British and European Standards, however, I would have expected the evidence in support of the claims associated with doors, dampers and penetrations to cite the most applicable standards for testing.

240 It should be recognised that the PCSR does identify the need to demonstrate that any penetrations are required to provide the same fire resistance as the barrier in which they are located and that this approach is consistent with my expectations. However, given that the standards and guidance cited as the supporting evidence is not consistent with the testing and criteria I would expect to see for items such as the doors and penetrations, an Assessment Finding (**AF-AP1000-IH-01**) (see Annex 1) has been raised to ensure that the various penetrations are specified appropriately and meet the overall

claim that they will provide an equivalent degree of fire resistance to the barrier in which they are installed.

241 The quoted standard for the fire dampers is an accepted standard for the design and installation of fire dampers for industrial practices. My expectations, however, in line with the single failure criterion detailed within the Safety Assessment Principles, SAP EDR.4, are that further measures may be required over and above those expected within the European Standards, specifically associated with the application of the single failure criterion to dampers which pass through nuclear significant hazard barriers. The PCSR identifies this as a shortfall and Westinghouse are currently undertaking a review of all fire dampers within the AP1000 design to ensure that the requirements of the Internal hazards safety case are met. Given that the outcome of the review may result in changes to the design for the HVAC and fire dampers a further GDA Issue Action (**GI-AP1000-IH-01.A2**) has been raised as part of the broader GDA Issue relating to the substantiation of internal fire safety case.

4.3.3.3 Conclusions

242 Whilst the PCSR recognises the need for penetrations within barriers to be adequately protected against the potential for fire spread, it does not provide reference to the correct standards with which the penetrations should be qualified in all cases. This is a relatively minor point for clarification that can be captured through the issue of an Assessment Finding as it is more associated with the specification for penetration sealing rather than a fundamental concern with the design. The approach taken to the analysis of fire dampers may be in line with my expectations but as the analysis was not provided by the time of writing this report it is not possible to assess and as such, a GDA Issue is warranted.

243 The following Assessment Finding has been raised associated with the specification for barrier sealing:

AF-AP1000-IH-01 – *The licensee shall, during the specification of the barrier penetrations as part of the detailed design studies, provide evidence to support that the method of barrier sealing is able to meet the 3 hour fire resistance requirements for insulation and integrity in accordance with the requirements stated within the PCSR.*

244 The Assessment Finding above should be addressed as part of the following procurement and construction generic milestone for assessment findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning

245 As part of the wider GDA Issue relating to internal fire, the following GDA Issue Action has been raised associated with the need to provide substantiation of the fire dampers installed within the AP1000 design:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Civil Engineering		
GDA Issue Reference	**GI-AP1000-IH-01**	**GDA Issue Action Reference**	**GI-AP1000-IH-01.A2**
GDA Issue Action	Provide the substantiation of the approach taken to the design and installation of fire dampers claimed within the AP1000 PCSR. This may include a multi-legged argument consisting of the following factors: • Details of the design approach to the installation of fire dampers within the AP1000 design. • The consideration of the single failure criterion. • Reference to the appropriate codes and standards which demonstrate the fire dampers installed will meet the requirements for 3 hours fire resistance both in terms of integrity and insulation. • Provisions associated with the application of any passive fire protection to ensure that the dampers meet insulation requirements as detailed within point 3 above.The approach taken to the control of the fire dampers both in terms of detection driven oper ensuring that full divisional segregation is met. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

246 The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.3.4 Cable Segregation and Separation

247 Cable segregation and separation was identified within the Step 3 Internal Hazards Assessment Report as requiring further assessment during Step 4 adequate arguments and evidence were not presented within the PCSR. This concern was to be addressed through the issue of the Internal Hazards Topic Report. As mentioned previously both the PCSR and Internal Hazards Topic Report have been used as the basis for the assessment within Step 4.

4.3.4.1 Scope of Assessment Carried Out

248 The scope of the assessment undertaken during Step 4 was to consider the arguments and evidence associated with the claims made relating to cable separation and segregation.

4.3.4.2 Assessment

249 The principles for cable segregation and separation stated within the PCSR are based upon a combination of fire resistant construction through the use of fire barriers, enclosures, and physical separation. This approach is consistent with my expectations

and the PCSR and Internal Hazards Topic Report considers cable routing within areas in detail. There are claims made within the PCSR and Topic Report associated with the following aspects of cable segregation and separation which were subject to further assessment during Step 4, namely:

- Cable tray combustible loadings; and
- Cable tray enclosures and passive protection.

250 Each of these areas has been subject to detailed assessment during Step 4.

4.3.4.2.1 Cable Tray Combustible Loadings

251 The PCSR states that cable tray insulation is selected to meet Institute of Electrical and Electronic Engineers (IEEE) and British Standards

252 Within the PCSR it is stated:

"As a minimum, the insulating and jacketing material for electrical cables is selected to meet the fire and flame test requirements of References 11.25 and 11.26, as discussed in the EDCD [Ref. 11.4, Appendix 9A] and appropriate BS codes of practice."

"Power cables are segregated from instrumentation cables to minimise the potential for cables to initiate fire. The cable loading of each tray will be fixed at 30 percent to limit the combustible load [Ref. 11.31]. Safety management procedures will be developed to ensure that cable tray loadings are managed. Evidence of such measures will be presented as part of the detailed design phase and will become part of the safety management procedures developed as part of the site-specific licensing."

253 This approach to managing the combustible loading on cable trays is a good approach to take to ensuring that the potential fire load does not have a detrimental effect on the claims made upon the barriers in place and also on any justification of fire separation. As a result reference 11.31 of the PCSR, *"Raceway Filling Report Auxiliary Building Elevation 66' 6"*, APP-1210-ERR-001 (Ref. 41) was subject to further assessment.

254 The report provides comprehensive information relating to the methodology applied to the analysis undertaken to demonstrate that the cable trays fill will be less than 30% full. The approach taken is to consider the loads required for each of the systems to be fed via the 66'6" level, the assignment of cable trays for those loads in question, the specific sizing of the cable trays in question and whether the proposed loading for the sizing of the cable trays is feasible. The approach to the analysis appears to be comprehensive and I believe this to be a valuable task in demonstrating that the barriers will not be threatened should the cable tray fill be assessed and managed in this way. The report details the filling limits for differing types of tray and are included in Table 3, below.

Table 3: Cable Tray Filling Limits

Tray usable Depth (inches)	Z Tray Filling Criteria	XA Tray Filling Criteria	XB Tray Filling Criteria	Conduit Filling Criteria
3.000	40%	40%	100%	53% (1 cable) 31% (2) 40% (over 2)

255 In addition, the report states, *"XA filling criteria has been trying to be kept below 30%, that is, more restrictive than the one specified on the Raceway Design Criteria"*. This does

not appear to be consistent with the claim made within the PCSR that cable tray fill is kept below 30%, whereas the report seems to identify this as a desirable fill percentage and that the limit is 40%. In addition, within Appendix A of the report, the detailed information relating to the cable tray fill percentage derived from the specific cables identifies a number of cable trays where the percentage full is in excess of 30% for XA cable trays. However, in all situations the cable fill criteria for XA cables never exceeds 40%.

256 The effect of the percentage fill of the cable trays between 30% and 40% may not have a significant impact on the overall safety case for internal fire; however, the claim within the PCSR associated with a maximum fill of 30% cannot be made for a number of cable trays. In addition, the PCSR does not differentiate between the different cable trays and Appendix A highlights cable trays as part of the XB criteria that are significantly higher than 30% and in many cases between 70-80%. Again, given the size of the cable trays for XB cables, this may not be a concern but as the PCSR does not differentiate between the cable trays the claim in this area is not substantiated.

257 TQ-AP1000-1272 requested details of any changes to the claims, arguments and evidence within the Consolidated PCSR from Revision A of the PCSR be provided and one of the areas is associated with providing clarity in the aforementioned statement. Westinghouse has identified this inconsistency between the PCSR and the reference document within the response to TQ-AP1000-1272 and TQ-AP1000-1282 states that the following text will be included within the next revision of the PCSR:

"Power cables are segregated from instrumentation cables to minimise the potential for cables to initiate fire. The cable loading of each type of tray will be fixed to limit the combustible load (Ref. 11.31). The usable tray depth is limited to 7.62 cm (3 inches). Correspondingly, the Z tray filling criteria is 40%; XA tray criteria, 40%, and XB tray criteria, 100%. Further, the conduit filling criteria is 53% (1 cable), 31% (2 cables), and 40% (over 2 cables). Safety management procedures will be developed to ensure that cable tray loadings are managed. Evidence of such measures will be presented as part of the detailed design phase and will become part of the safety management procedures developed as part of the site-specific licensing."

258 Given the detailed approach taken in the assessment of cable tray combustible loadings undertaken I am satisfied that the evidence associated with cable tray filling limits can be addressed through an Assessment Finding. The Assessment Finding (**AF-AP1000-IH-02**) (see Annex 1) has been identified which requires the evidence of the management procedures to ensure that cable tray loadings are managed as part of the site specific PCSR.

259 It is recognised that the above analysis, referenced from the PCSR, is only associated with the 66'6" level of the Non-RCA area of the Auxiliary Building and as a result an Assessment Finding has been raised identifying the need for this analysis to be undertaken for all cable trays that contain cabling which performs a Class 1 safety function, with the exception of those cable trays contained within fire rated enclosures or that are provided with passive fire protection. (**AF-AP1000-IH-03**) (see Annex 1).

4.3.4.2.2 Cable Tray Enclosures and Passive Protection

260 PCSR Section 11.4.3.4. states:

"Class 1 cables are supported with lidded, galvanized-steel bottom trays, which provide protection from ignition sources arising from damage to other cables. Supports for cable

trays in the NI are C-I. C-I supports are also used for seismic Category II (C-II) areas to minimise their potential to become damaged and present potential ignition sources in the event of a DB earthquake. To minimise the risk of a fire in a cable of one of the Class 1 electrical divisions acting as an ignition source to cables of other electrical divisions, cables of different divisions are routed in separate raceways, which are themselves physically separated. Within the NI, some Class 1 cables of different divisions are protected from fire using passive protection means in the form of insulated steel-composite materials.

These measures ensure that common ignition sources are adequately controlled."

261 There is further information relating to the protection of cable trays and the application of passive protection within Section 11.4.4. of the PCSR which states that there are a number of cable ducts protecting Class 1 electrical cables which are contained within 3 hour fire resistant enclosures. As these are :

"Within the NI, there are a number of cable ducts and chases protecting Class 1 IDS cables, including a 3-hour fire-resistant enclosure for the Division B and D penetration room within the containment building. The Class 1 IDS electrical cables that are located in or pass through an area, but are specifically separated from it by 3-hour fire barriers (e.g., in a cable chase), are considered adequately protected and are not considered as part of the area. The requirement for additional local passive protection measures will be reviewed as the design progresses as part of the site-specific licensing process."

262 I am content with the approach taken to the segregation of cables from different trains using fire protected enclosures, however the need for substantiation of the enclosures is captured as part of the assessment undertaken within Section 4.3.2 of this report relating to nuclear significant fire barriers and as a result are not considered further within this section.

263 I am also content with the application of passive fire protection to cables in order to provide segregation within the limited areas of commonality within the design and as a means by which to reduce their contribution to fire within a room or area. However, as the identification of the specific locations of protection to cable routes has not been identified, and given that the PCSR reflects this aspect as requiring review as the design progresses, an Assessment Finding has been raised (**AF-AP1000-IH-04**) (See Annex 1). I am content with this aspect of the cable protection being identified as an Assessment Finding as it is recognised that there will be aspects of the design that require further consideration associated with separation and segregation as well as the minimisation of combustible inventories within areas.

4.3.4.3 Conclusions

264 The detailed analysis that underpins the PCSR associated with cable tray filling, and ensuring that the cable trays will not be overfilled and contain cables of the incorrect designation and the approach to providing protection to cable trays is in line with my expectations.

265 Furthermore, the approach taken in relation to minimising the effects of incidents and minimisation of combustible inventories through good design practice, is consistent with SAPs EHA.14, and EHA.17 as well as the guidance within NS-G-1.7.

266 The following three Assessment Findings have been raised as a result of my assessment:

AF-AP1000-IH-02 – *The Licensee shall provide evidence of the management procedures to demonstrate that the cable tray loadings are managed to ensure that the fill limits as detailed within the PCSR as maintained below the requisite levels stated within the design.*

AF-AP1000-IH-03 – *The Licensee shall provide analyses in line with that undertaken within Westinghouse report, "Raceway Filling Report Auxiliary Building Elevation 66' 6", APP-1210-ERR-001 (Ref. 41) as part of the site specific PCSR for all cable trays that contain cabling which performs a Class 1 safety function, with the exception of those cable trays contained within fire rated enclosures or that are provided with passive fire protection.*

AF-AP1000-IH-04 – *The Licensee shall provide details of all cable routes provided with passive fire protection as part of the site specific PCSR and furthermore, explain the basis for the application of passive fire protection and the impact on nuclear safety of the aforementioned protection.*

267 The three Assessment Findings above should be addressed as part of the following procurement and construction generic milestones for assessment findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning

4.3.5 Exceptions to Segregation

268 There are some areas within Containment and sub-floor of the Main Control Room where due to the single location there is commonality in the cable routing of all four divisions, however, this is tackled through fire protection of the cables and providing the maximum physical separation distance between the cable routes.

4.3.5.1 Scope of Assessment Carried Out

269 The scope of the assessment undertaken during Step 4 was to consider the arguments and evidence associated with the claims made relating to exceptions to segregation in areas where physical fire barriers are not provided as well as to consider areas where claims are made on geographical separation. The focus of the assessment is principally within Containment and the Main Control Room given that these are the two areas where exceptions to segregation are known to exist.

4.3.5.2 Assessment

270 The divisional cables within the containment are separated both by distance and by the use of fire resistant cladding. The distance between the divisional cables is approximately 3.6 metres, however, given that the cables are also provided with fire and hazard protection (such as steam and moisture) through the use of fire resistant enclosures coupled with the very low fireloadings within Containment (i.e. no lubricating oil used for the Reactor Coolant Pumps) this distance is sufficient to ensure that fire involving one division separation train would not have a detrimental effect on any others within Containment. In addition the Fire Hazard Analysis, which was subject to assessment within Section 4.3.1 of this report, provides a detailed analysis of the potential threats to segregation within the Containment from the effects of fire. I am

satisfied that the safety case claims, arguments and evidence relating to exceptions to segregation within the Containment are acceptable.

271 The Main Control Room (MCR) is located at the north east corner of the non-radiologically controlled area of the auxiliary building. It provides operator monitoring and control functionality. Redundancy of equipment within the MCR is provided by that in the Remote Shutdown Room (RSR).

272 The MCR and RSR bring together equipment from the four divisions of the Class 1 electrical systems. Cables and their routes within the MCR and the RSR to essential plant monitoring devices are segregated to minimise the potential for spurious signals as a result of a fire in these rooms. This section considers the approach taken to minimising loss of more than one division within the MCR and considers the arguments presented demonstrating that this approach is acceptable.

273 There are cables and equipment located within the MCR from all four divisions. The arguments presented within the PCSR include:

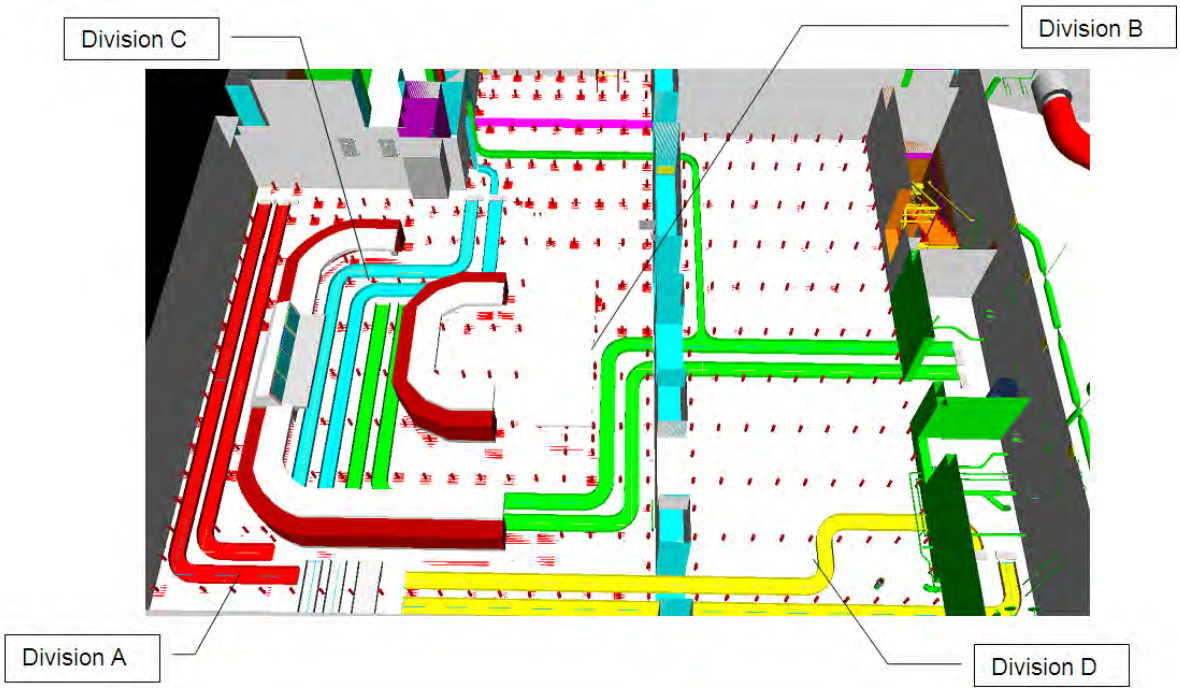
- Low fire risk due to limited combustible inventory and use of fibre optic cabling.
- Remote shutdown station contained within a separate 3 hour fire barrier with independent cable routes from SSCs important to safety.
- Isolation of all power within MCR through the use of a transfer switch such that spurious operation of SSCs important to safety is prevented.
- Permanently occupied area by trained personnel.
- Portable fire extinguishing capability.

274 The arguments presented above associated with low fire risk and the capability of the RSR have been subject to further assessment below.

4.3.5.2.1 Low Fire Risk Due to Limited Combustible Inventory and Use of Fibre Optic Cabling

275 Figure 1, below, illustrates the different divisional routes located beneath the MCR. It is important to note that the cable trays shown beneath the floors comprise the totality of the cable trays and not just the divisional separation groups (due to the use of fibre optics), which is significantly different to the existing UK reactor fleet where cable mezzanines beneath the MCR are generally very high fireload areas protected by fast acting suppression systems. In addition, there is redundancy applied within the design by virtue of the provision of the remote shutdown station, whose divisional separation cable trays do not pass through sub-floor of the MCR. Given the significantly reduced fireload inventory beneath the MCR arising from the use of fibre optic cable coupled with the local fire protection applied to the cable routes as well as the provision of the remote shutdown station where the divisional cables are not routed beneath the sub-floor of the MCR, the risk of fire or any other Internal hazards resulting in loss of more than one division due to failures attributed to the cable routing is ALARP.

Figure 1: 3D Computer Model Layout of the Cable Trays Beneath the MCR



4.3.5.2.2 RSR and MCR Transfer Capability

276 The remote shutdown room is contained within a separate 3 hour fire compartment west of the MCR and on the level below. The RSR is only operational should the MCR become untenable due to fire. The operators would make their way down a staircase from the MCR directly to the RSR. Within this staircase is a transfer set which is required to be switched from the MCR to the RSR. This transfer set serves to isolate power from the MCR to the RSR. This eliminates the potential for fire to result in spurious operation of plant systems and as the RSR has segregated and independent control and monitoring functions for safe shutdown, the requisite control and monitoring functions can be undertaken from there.

277 I am satisfied that suitable provisions exist for ensuring that plant control and monitoring functions can be achieved should the MCR become untenable due to fire.

4.3.5.3 Conclusions

278 I am satisfied that the exceptions to segregation within the AP1000 have been adequately captured and that sufficient analysis has been undertaken to demonstrate the claims made within the PCSR are substantiated.

279 There are no GDA Issues or Assessment Findings associated with this aspect of my assessment.

4.3.6 Spurious Operation and Common Cause Failure

280 Given the compact nature of the AP1000 design and the identification of areas where multiple trains are routed, consideration was given to the assessment of the potential for spurious operation and common cause failure.

281 The PCSR has a dedicated section that addresses the potential for such events and provides claims and arguments together with reference to the evidence.

4.3.6.1 Scope of Assessment Carried Out

282 The scope of the assessment undertaken during Step 4 was to consider the arguments and evidence associated with the claims made relating to spurious operation and common cause failure. The PCSR and the following reference document cited were subject to assessment during Step 4:

- *"AP1000 Fire Induced Multiple Spurious Actuation Report,"* APP-FPS-G1R-002" (Ref. 42)

4.3.6.2 Assessment

283 The design of the AP1000 deals with common cause failure and spurious operation by providing appropriate, segregation, separation and redundancy of safety systems to ensure that no Category A safety function will be compromised. The PCSR includes a number of statements on the design of the AP1000 in the prevention of common cause failure and spurious activation including the following:

284 Section 11.4.6 of the PCSR states "*In the event of a fire within any fire compartment forming part of the AP1000 plant (or fire zone within the containment building), it is pessimistically assumed that all SSCs fail within that area. In general, this might result in safety function(s) supported by the equipment within that fire compartment no longer being delivered and/or spurious actuations that may have a negative impact on plant safety. Therefore, in order to ensure that no safety functionality is lost, the AP1000 plant is designed such that:*

- *No single SSC failure can result in the failure to deliver the Category A safety functions (taking into account that there is a periodic need to take certain individual systems offline during operation in order to undertake maintenance activities).*
- *No spurious activation can cause erroneous actions that may have a negative impact on plant safety*.

285 Section 11.4.6.2 of the PCSR states that "*Fire-caused damage to electrical circuits is assumed to be capable of resulting in hot shorts, open circuits, and shorts to ground. The AP1000 plant PMS, PLS, and DAS have been designed to minimise the likelihood that spurious actuations will cause disruptions to plant operations in the event of a fire-induced fault. Details of the function and operation of the control systems are discussed in Chapter 6, Section 6.6.*

286 The PCSR provides an overview of the analysis work undertaken to demonstrate the spurious actuation as a result of fire is either not credible or that should it occur the consequences are such that it would not affect the delivery of Category A or supporting Category B functions. Further assessment has been undertaken of the Automatic Depressurisation System (ADS) Valve Actuation and the substantiation of this system in relation to spurious operation.

287 The PCSR and the reference, *"AP1000 Fire Induced Multiple Spurious Actuation Report"*, APP-FPS-G1R-002 have been used to inform the assessment of the above two systems.

288 This assessment has focused on the substantiation detailed within the PCSR to support the claim that spurious operation of the ADS would not occur as a result of a single fire.

The analysis undertaken in support of the PCSR concludes that either spurious actuations do not occur, or the consequences are such that they do not prevent delivery of the Category A safety function and the Category B support functions.

289 Section 11.4.6.2. of the PCSR states:

"The ADS valves are not considered to be high-low pressure interface valves when postulating spurious actuations following a fire. The concern is that the spurious opening of two or more isolation valves forming the boundary between the RCS and a low-pressure system could lead to damage to the low-pressure system and a loss of coolant outside the containment. Since the ADS valve actuation cannot damage a low-pressure system, and since the system is entirely within containment, the ADS valves do not represent a high-low pressure interface."

290 Reference 41, provides further information relating to this statement and highlights that the "concern" stated within the PCSR arises from a US NRC Generic Letter 81-12 (Ref. 43), in which the relevant section of the letter states:

"2. The residual heat removal system is generally a low pressure system that interfaces with the high pressure primary coolant system. To preclude a LOCA through this interface, we require compliance with the recommendations of Branch Technical Position RSB 5-1. Thus, this interface most likely consists of two redundant and independent motor operated valves. These two motor operated valves and their associated cable may be subject to a single fire hazard. It is our concern that this single fire could cause the two valves to open resulting in a fire-initiated LOCA through the subject high-low pressure system interface. To assure that this interface and other high-low pressure interfaces are adequately protected from the effects of a single fire, we require the following information:

A. Identify each high-low pressure interface that uses redundant electrically controlled devices (such as two series motor operated valves) to isolate or preclude rupture of any primary coolant boundary.

B. Identify the device's essential cabling (power and control) and describe the cable routing (by fire area) from source to termination.

C. Identify each location where the identified cables are separated by less than a wall having a three-hour fire rating from cables for the redundant device.

D. For the areas identified in item 2.C above (if any), provide the basis and justification as to the acceptability of the existing design or any proposed modifications."

291 Although the ADS is not considered a high/low pressure interface, the potential for spurious actuation of the ADS valves was subject to analysis as part of the AP1000 design given the potential for depressurisation of the RCS through the passive system, and hence consideration was given to the potential for spurious operation of the valves included within this system.

292 The basis for claiming that fire would not result in a spurious operation of the valves associated with the ADS involves arguments associated with:

- The segregation of the four PMS command and interface cabinets between Divisions A and C, and Divisions B and D;

- The remote location of the Stage 4 ADS valves;
- The need for two separate commands from the system in order to actuate the valves (ARM and FIRE commands); and,
- The normally de-energised nature of the manual Diverse Actuation System (DAS).

293 This assessment has considered the arguments made in relation to the location of the cabinets and the segregation provided and not the detailed design of the systems from a control and instrumentation (C&I) perspective as this has been considered as part of the Step 4 Control and Instrumentation assessment of the Westinghouse AP1000 (Ref. 44).

294 There is 3 hour fire segregation between the command and interface cabinets for Divisions A and C, and Divisions B and D. The Division A and C cabinets are located within the Division C electrical room, however, they are located within different locations within that room. Similarly, the Division B and D cabinets are located within the Division B electrical room with the cabinets being located within separate areas of that room. The arguments for the systems being within the same room involve claims that failure would require simultaneous multiple hot shorts in different trains and the low likelihood of this as a mechanism. The potential for spurious operation within specific systems, or parts thereof, has been addressed as part of the Step 4 Control and Instrumentation assessment of the Westinghouse AP1000.

295 The PCSR states that there is no reliance on operators to perform actions to isolate aspects of control and power in the event of a fire within any of the rooms contained ADS control and any actions are identified as defence in depth. One of the defence in depth actions associated with an ADS Stage 4 valve is addressed within the PCSR which states:

"Prevention of a single spurious signal to the ADS Stage 4 valve as a result of a fire affecting one PMS interface cabinet for a given electrical division can be avoided by a defence-in-depth operator action that can remove power from the affected fire zone. Again, these actions (which are described in detail in the following paragraphs) are not relied upon to maintain plant safety, and failure of the operator to carry out these actions does not lead to further spurious actuations within other electrical divisions."

4.3.6.3 Conclusions

296 I am satisfied with the claims presented for the segregation provided utilising 3 hour fire barriers, however, there do not appear to be claims made on the separate location of the cabinets within the rooms that contain Divisions A and C, or Divisions B and D. Furthermore there are no claims made on the fire resistance of the cabinets contained within those rooms. Therefore, the claims appear to be solely attributable to the preclusion of spurious operation through the C&I design which has been considered as part of the Step 4 Control and Instrumentation assessment of the Westinghouse AP1000.

297 In addition, the PCSR does not place any claims upon operators to undertake action in the event of fire and all operations undertaken are specifically identified as defence in depth.

4.3.7 Fire Protection Systems

298 The nuclear safety claims associated with the Fire Protection System (FPS) were subject to assessment during Steps 2 and 3, however, there remained a lack of clarity associated

with the potential claims made upon the system to perform a nuclear safety function. The Step 3 Internal Hazards Assessment stated:

"…..subsequent discussions have been held with WEC who believe that there are no nuclear safety claims associated with any of the fire protection systems installed as part of the AP1000 design. As there currently appear to be claims on the FPS associated with fire spread beyond compartments and within containment within the TQ response, further assessment of these claims is to be undertaken as part of the Step 4 assessment."

299 The assessment during Step 4, therefore, considered whether such claims made on the Fire Protection are indeed required to ensure nuclear safety.

4.3.7.1 Scope of Assessment

300 The assessment has focused on statements made within the PCSR and Internal Hazards Topic Report associated with the FPS installed as part of the AP1000 design.

4.3.7.2 Assessment

301 Section 11.4.9 of the PCSR states:

"No claim is made on the firefighting system within the AP1000 design. Instead, these systems and the fire detection and alarm system are provided to minimise the consequences of fire and to limit fire spread. In addition, the firefighting systems are used to protect Class 2 and 3 equipment; keeping the Class 2 and 3 systems operational minimises the demand placed on Class 1 systems."

302 The FPS is identified as providing further mitigation and no nuclear safety claim is associated with the system. Furthermore, the PCSR states:

"The fixed firefighting system is not relied upon to protect Category A safety functions; however, it is used to protect Class 2 systems and reduce the demand on the Class 1 systems. Seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake. In addition, the CIVs [Containment Isolation Valves] and associated penetration piping for the FPS are Class 1 and C-I. The FPS is not required to remain functional following a plant accident or the most severe natural phenomena, except as stated for an earthquake."

303 It is recognised that there are portions of the FPS that pass into Containment and in order for the function of the Containment to be assured, the containment isolation valves are appropriately rated to ensure that they do not fail during a seismic event. The claims made in this situation are to ensure the integrity of the Containment. However, I am uncertain over the potential claims made associated with the final statement within the above paragraph relating to the implication that the FPS requires to be functional following a seismic event which appear to be inconsistent with the statements made within Section 11.4.9 of the PCSR. A TQ (TQ-AP1000-1272) requested details of any changes to the claims, arguments and evidence within the Consolidated PCSR from Revision A of the PCSR be provided and one of the areas is associated with providing clarity in the aforementioned statement. The TQ response states:

"Augmentation of existing statement on seismic design requirements applied to the fixed fire fighting standpipe. ND highlighted this in a Level 3 meeting."

304 The TQ response stated that there were to be no changes to be made to the claims, arguments and evidence in this situation, however, as mentioned previously, there is uncertainty over the whether there are claims being made on the functionality of the FPS in the event of a seismic event. A further confirmatory TQ has been raised (TQ-AP1000-1279) requesting Westinghouse to confirm whether the Fire Protection System is required to be functional, i.e. provide water for fire fighting or containment cooling, in a seismic event.

305 The response to TQ-AP1000-1279 confirmed that there were no nuclear safety requirements for the FPS and stated:

"The fire protection system (FPS) is not credited nor required as part of the safety case to remain functional following a plant accident or occurrence of the most severe natural phenomena. However, portions of the FPS are designed to provide water to hose stations for manual firefighting in areas containing safe shutdown equipment following a safe shutdown earthquake. As a result, special seismic design requirements have been applied to portions of the standpipe system design located in those areas containing such equipment.

As a further consistent indication of the FPS classification, there are no identified operator actions required to protect Category A safety functions from fire via use of the manual hose stations."

4.3.7.3 Conclusions

306 I am satisfied that there are no nuclear safety claims made on the fire protection system in order to protect Category A safety functions and no associated operator actions required to be undertaken other than for risk mitigation.

307 No GDA Issues or Assessment Findings are therefore required as part of this aspect of my assessment.

4.3.8 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

308 This section details some of the standards, guidance and relevant good practice utilised in my assessment of internal fire undertaken on the AP1000 design. It cites key aspects of the standards and guidance used in order to inform the judgements made within my assessment and to underpin the need for either GDA Issues or Assessment Findings.

309 The internal fire aspects of the AP1000 design is consistent with TAG, T/AST/014, which states:

"In order that items important to safety will have the level of reliability required to meet the safety goals, the licensee must consider the possibility of single random failures, common cause failures, simultaneous and consequential events and unavailability of SSCs due to maintenance activities. Common causes include both SSC failures and effects of internal hazards such as fire. The appropriate level of reliability of essential safety functions may be achieved by incorporating redundancy within single trains and/or segregation and diversity between trains."

310 The need for redundancy, diversity and segregation are captured within SAPs EDR.2:

Engineering principles: design for reliability	Redundancy, diversity and segregation	EDR.2
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.		

311 The consideration of the basis for the redundancy in systems is captured within SAP EHA.5:

Engineering principles: external and internal hazards	Operating conditions	EHA.5
Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.		

312 The need for quantitative analysis of internal hazards is addressed within SAP EHA.14:

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

313 The above SAPs are addressed within the AP1000 design through the provision of multiple redundant and segregated trains that have been designed such that the potential for loss of more than one train does not occur as a result of a single fire within the facility. This is, however, dependent on the GDA Issue relating to the substantiation of the fire barrier (**GI-AP1000-IH-01.A1**).

314 With regard to the analysis of other potential effects associated with internal hazards, T/AST/014 states:

"In order that items important to safety will have the level of reliability required to meet the safety goals, the licensee must consider the possibility of single random failures, common cause failures, simultaneous and consequential events and unavailability of SSCs due to maintenance activities. Common causes include both SSC failures and effects of internal hazards such as fire. The appropriate level of reliability of essential safety functions may be achieved by incorporating redundancy within single trains and/or segregation and diversity between trains."

315 This is also captured within the SAPs, SAP EHA.6 states:

Engineering principles: external and internal hazards	Analysis	EHA.6
Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.		

316 The approach taken to the design of the AP1000 considers such events and the provisions in place are broadly in line with the SAPs, however, given the current uncertainty over the approach to the application of the single failure criterion for fire dampers that pass through nuclear significant hazard barriers, there is a need for further

evidence within this area. This has been captured as a GDA Issue (**GI-AP1000-IH-01.A2**).

317 The approach to segregation within the AP1000 design is consistent with the IAEA guidance document, NS.G.1.7, which states within the section entitled, *"General Concepts"*:

"Structures, systems and components important to safety are required to be designed and located, consistent with other safety requirements, so as to minimize the likelihood and effects of internal fires and explosions caused by external or internal events. The capability for shutdown, removal of residual heat, confinement of radioactive material and monitoring of the state of the plant is required to be maintained. These requirements should be met by the suitable incorporation of redundant parts, diverse systems, physical separation and design for fail-safe operation…"

318 In addition, it states:

"….*the overall purpose of fire barriers in nuclear power plants is to provide a passive boundary around a space (e.g. a fire compartment) with a demonstrated capability to withstand and contain an expected fire without allowing the fire to propagate across to, or otherwise cause direct or indirect damage to, materials or items on the side of the fire barrier not exposed to the fire. The fire barrier is expected to perform this function independently of any fire extinguishing action*."

319 IAEA NS-G-1.7 states within paragraph 3.17:

"Fire cells are separate areas in which redundant items important to safety are located. Since fire cells may not be completely surrounded by fire barriers, spreading of fire between cells should be prevented by other protection measures. These measures include:

- *The limitation of combustible materials;*
- *The separation of equipment by distance, without intervening combustible materials;*
- *The provision of local passive fire protection such as fire shields or cable wraps;*
- *The provision of fire extinguishing systems.*

Combinations of active and passive measures may be used to achieve a satisfactory level of protection; for example, the use of fire barriers together with an extinguishing system."

320 As has been identified, there are areas where full compartmentation has not been achieved and the fire cell approach has been adopted within the AP1000 design. The approach taken with the design is consistent with my expectations and the expectations of the IAEA guidance.

321 For cable routing and segregation, NS-G-1.7 state within paragraphs 4.7 and 6.14 respectively:

"*Cables should be laid on trays made of steel, installed in steel conduits or placed in other structurally acceptable and non-combustible cable supports. The distances between power cables or cable trays should be sufficient to prevent the cables from heating up to unacceptably high temperatures. The electrical protection system should be designed so that the cables will not overheat under normal loads or transient short circuit conditions [10, 11]. Care should be taken to ensure that cables serving items important to safety are not routed over designated storage areas or other such areas of high fire hazard."*

"Cabling for redundant safety systems should be run in individual specially protected routes, preferably in separate fire compartments, and no cables should cross between redundant divisions of safety systems. As outlined in para. 3.15, exceptions may be necessary in certain locations such as control rooms, cable spreading rooms and the reactor containment. In such cases, the cables should be protected by means of qualified fire rated barriers (e.g. cable 37wraps). Fire extinguishing systems or other appropriate means may be used, with justifications made in the fire hazard analysis."

322 I am satisfied that the above aspects of cable routing and segregation have been captured within the AP1000 design and where there are areas of commonality, namely, the MCR, the RSR, and the Containment that the case is underpinned by detailed analysis substantiation through the fire hazard analysis in these instances.

323 Complimenting the statements made within ND and IAEA guidance and WENRA Reference Level S: Protection against internal fires, states within its basic design principles:

- *SSCs important to safety shall be designed and located so as to minimize the frequency and the effects of fire and to maintain capability for shutdown, residual heat removal, confinement of radioactive material and monitoring of plant state during and after a fire event.*
- *Buildings that contain equipment that is important to safety shall be designed as fire resistant, subdivided into compartments that segregate such items from fire loads and segregate redundant safety systems from each other. When a fire compartment approach is not practicable, fire cells shall be used, providing a balance between passive and active means, as justified by fire hazard analysis.*

324 The guidance also recommends:

- *A fire hazard analysis shall be carried out and kept updated to demonstrate that the fire safety objectives are met, that the fire design principles are satisfied, that the fire protection measures are appropriately designed and that any necessary administrative provisions are properly identified.*
- *The fire hazard analysis shall be developed on a deterministic basis, covering at least:*
  - *i) For all normal operating and shutdown states, a single fire and consequential spread, anywhere that there is fixed or transient combustible material;*
  - *ii) Consideration of credible combination of fire and other PIEs likely to occur independently of a fire.*

325 In addition, existing UK nuclear power generation facilities apply a similar approach to ensuring that there is adequate redundancy and segregation in place to ensure that the design basis stated above is met.

326 The approach taken for the analysis undertaken for AP1000 is broadly in line with that observed within ND guidance, international standards and guidance, and relevant national and international good practice.

4.3.9 Conclusions of the Internal Fire Assessment

327 I am satisfied that a thorough and robust approach to the design of the AP1000 has been undertaken in relation to internal fire and the expectations detailed within standards and guidance are broadly met. The GDA Issues and Assessment Findings within the internal

fire area are largely associated with the provision of adequate substantiation and evidence that is currently not fully explained and detailed within the PCSR.

4.4 Nuclear Directorate Assessment of Internal Flooding

4.4.1 Scope of Assessment Carried Out

328 The Step 3 Internal Hazards Assessment Report for the AP1000 identified the need for further assessment of the PCSR associated with internal flooding. This was due to the uncertainty associated with the claims presented during Step 3. The approach to addressing the safety case in this area was through the production of an Internal Hazards Topic Report, which was not subject to detailed assessment during Step 3 given that it was issued too late in the process to allow for sufficient assessment.

4.4.2 Assessment

329 During Step 4, Westinghouse identified a number of outstanding aspects of the case, namely associated with the identification of barriers claimed to prevent flooding affecting more than one train of protection, the potential flood heights and shortfalls associated with the calculation of the potential flood volumes. Westinghouse proposed issuing a revised safety case for internal flooding towards the end of Step 4. This report was not provided in time for sufficient assessment to be undertaken during Step 4.

4.4.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

330 The SAPs, EHA.14 and EHA.15 state:

Engineering principles: external and internal hazards	**Fire, explosion, missiles, toxic gases etc – sources of harm**	**EHA.14**
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

331 This SAP calls for potential flood sources to be specified quantitatively and their potential source of harm to the nuclear facility assessed.

Engineering principles: external and internal hazards	**Fire, explosion, missiles, toxic gases etc – effect of water**	**EHA.15**
The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.		

332 The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water.

333 Furthermore, IAEA Safety Guide, NS-G-1.11 states:

"*All possible PIEs [potential initiating events] should be carefully identified. The best approach is to base the list of PIEs on a list of SSCs and then to identify all the possible*

sources of liquid (water in the case of pressurized water reactors and boiling water reactors), including sources in other rooms. This identification should be supported by room by room walk-downs.

For each PIE, P1 should be determined, with account taken of possible human errors.

For all PIEs, unless P1 is acceptably small, a liquid level as a function of time should be determined not only for the room with the source of the liquid but also for all rooms to which the liquid could spread (through doors, pipe conduits or cracks in walls or floors). In the case of breaks in pipes connected to tanks or pools, account should be taken of possible siphoning effects, which can increase the amount of liquid drained. Possible blocking of drain holes by debris should be taken into account if this would lead to more severe conditions. In determining the liquid level using a volume–height relation, the as-built status of the room should be used. The possible collection of liquid in upper parts of the room (e.g. in cable trays) should also be analysed. In some cases it may be necessary to analyse the flooding also with regard to the transport of objects and/or small particles to undesired locations. A typical example is the blockage of the strainers of the emergency core cooling system. Isolation debris, corrosion particles and even human hair can be transported by water and can block the strainers.

Reduction in the probability P2 of SSCs being affected by flooding can be achieved, for example, in the layout of the plant. Effective physical separation of redundant systems may in this case mean vertical separation. The SSCs can be located on a pedestal that is higher than the maximum possible flooding level. If this is not possible, a barrier (either a wall around the component or a complete enclosure) can be used. It should also be ensured by all available means that flooding (unless it is intentional flooding as a design feature) is mitigated as soon as possible and its spreading to unfavourable regions is prevented (e.g. by means of suitable thresholds). Means that can be used to mitigate flooding include:

(a) Appropriate design (isolation valves on potentially hazardous pipes, drains and pumps);

(b) Detection systems (flood warnings);

(c) Procedures (operational and/or emergency procedures).

For all actions taken in mitigation, the likelihood of success should be carefully evaluated. In case of any doubt, their failure should be assumed in the analysis. In the deterministic approach, the most severe single failure should always be assumed."

334 Given that the PCSR and the potential flood sources together with the associated claims on the barriers, sumps and drainage etc. are unclear due to the late delivery of the revised safety case for internal flooding, the principles within the SAPs and the approach taken within IAEA guidance have yet to be assessed.

4.4.4 Conclusions of the Internal Flooding Assessment

335 The revised safety case for internal flooding had not been issued at the time of writing this report and as a result the following GDA Issue **GI-AP1000-IH-02** has been raised seeking the revised internal flooding safety case:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-02**	**GDA Issue Action Reference**	**GI-AP1000-IH-02.A1**
GDA Issue	There is a need to provide an updated internal flooding safety case as there are inconsistencies associated with claims made on barriers, drains and sumps, and flood calculations.		
GDA Issue Action	Provide an updated internal flooding safety case that considers the claims, arguments and evidence associated with internal flooding. As part of the production of the aforementioned case there is a need to consider the following aspects within the safety case: • All potential unmitigated flood sources taking into account bounding flood sources and volumes. • The barriers claimed to provide segregation of safety significant SSCs in the event of internal flooding. • Any claims made on drainage systems, sumps, drains, flow paths etc and arguments and evidence provided to demonstrate that they will be available for postulated internal flooding events. • Any claims made on pressure relief panels and compartment vents need to supported by arguments and evidence to demonstrate that they will be available for postulated internal flooding events. • Any ALARP claims made on operator actions in relation to the mitigation of potential flood events rather than assuming operator success as part of the deterministic case. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

4.5 Nuclear Directorate Assessment of Pressure Part Failure

336 During Step 3 of the GDA process a high level assessment of the main principles in place against the internal hazards of pipe whip, including jet impingement and spray was undertaken. The detailed claims and arguments associated with these hazards were not subject to assessment during Step 3 and as a result have been subject to assessment during Step 4. The Step 4 assessment has also considered the supporting evidence to the claims and arguments made within this area.

4.5.1 Scope of Assessment Carried Out

337 The assessment has focused on the principal claims, arguments and evidence associated with the safety case as detailed within the PCSR for pressure part failure. The approach taken to the assessment of principles in the first instance allowed for more detailed sampling to be undertaken of the areas where pressure part failure has the potential to result in threats to either multiple trains of protection or loss of plant and equipment performing a nuclear safety significant role.

4.5.2 Assessment

338 The PCSR presented the analysis of postulated pressure part failure events on a floor-by-floor and room-by-room basis, depending upon the relative location of safety-related equipment. The analysis firstly identified potential hazard sources (e.g. postulated ruptures, leak-before-break and no break zones), and secondly evaluated the effects on equipment (e.g. pipe whip, jet effects, environmental effects, and etc.)

339 The analysis was focused on those areas containing the safety Class 1 SSCs. Consideration of pressure part failures in other locations was limited to a demonstration that the nuclear island was adequately protected from postulated pressure part failures by distance and / or physical barriers.

340 The safety design methodology described in the PCSR (Section 11.6.2) follows two distinct design approaches; pressure part failure inside containment and outside containment. Within containment the approach applied includes design and qualification of high pressure SSCs, a combination of separation and use of barriers to minimise the potential to affect Class 1 SSCs, and quantification of SSCs to operate under harsh environmental conditions. Outside containment the effects of a pressure part failure were limited to a single room through the use of structural barriers.

341 Section 11.6.5.2 of the PCSR stated the preferred design approach, which is as follows:

"*Protection against the dynamic effects of pipe failures is provided by physical separation of systems and components, barriers, equipment shields, and pipe whip restraints. The precise method chosen depends largely upon considerations such as accessibility and maintenance.*

The preferred method of providing protection is by separation (see Section 11.6.5.3).When separation is not practical, pipe whip restraints are used (see Section 11.6.5.4). Barriers or shields are used when neither separation nor pipe whip restraints are practical (see Section 11.6.5.5). This protection is not required when piping satisfies leak-before-break criteria."

342 Section 11.6.5.5. of the PCSR described the provision of barriers and shields, which are provided to protect against jet impingement, and states:

"Protection requirements are met through the protection afforded by walls, floors, columns, abutments, and foundations. Where adequate protection does not already exist as a result of separation, separating structures such as additional barriers, deflectors, or shields are provided to meet the functional protection requirements.

Barriers and shields include walls, floors, and structures specifically designed to provide protection from postulated pipe breaks. Barrier and shield designs are based on elastic methods and the elastic-plastic methods for dynamic analysis included in Reference 11.85. Design criteria and loading combinations are according to the EDCD [Ref. 11.4, Sections 3.8.3 and 3.8.4]."

343 Section 11.6.4.1 of the PCSR, which presents the results of the pipe whip analysis within the Containment / Shield Building, identifies the following areas where pipe whip cannot be precluded:

- ADS valve areas;
- SG compartments;
- Upper pressuriser compartment;

- Maintenance floor and mezzanine level;
- And pipe chase to CVS equipment room.

344 The PCSR states "*that mitigation is provided in the form of pipe whip restraints or barriers or shields.*" Based on the design approach described above, barriers and shields are provided to protect against jet impingement, or in the event when neither separation nor pipe whip restraints are practical. The PCSR referred to Table 11-4, where pipe whip restraints are claimed to mitigate the consequences, whilst barriers or shields claimed against these scenarios are captured as part of the civil design, namely Chapter 16 of the PCSR.

345 Chapter 16 of the PCSR was reviewed to determine the claims made on the barriers and shields in place that were claimed to provide protection to class 1 SSCs. Chapter 16 Section 16.1.5.2 states:

"The requirements have been identified for the walls and floors forming the rooms contained within the nuclear island to act as barriers against relevant internal hazards. This information has been presented in the form of a barrier matrix [Ref. 16.9]. PCSR chapter 11 identifies claims with respect to the civil engineering structures. The civil engineering design addresses loads arising from the following internally generated hazards:

- *Blast pressure*
- *Water pressure*
- *Missiles*
- *Pipe rupture*

The justification of adequately designed fire barriers and the provision of barriers for radiation shielding are considered in Chapters 11 and 24 of this PCSR, respectively."

346 As can be noted from the information above, Chapter 16 refers back to Chapter 11 of the PCSR and the AP1000 Barrier Matrix for information on the claimed barriers and does not identify any claims made on specific barriers or shields nor does it include any justification for the claims made on the civil structures.

347 Section 16.5 of the PCSR also details the applicable codes, standards and methodologies, and within sub sections 16.5.1.3 and 16.5.1.4 there is reference made to the justification of missile barriers and evaluation of postulated pipe rupture, respectively. Within the section relating to missile, there is reference made to design codes used in the construction of missile barriers, but no reference to the barriers that are to be claimed for the protection against such missiles. The section on postulated pipe failure makes reference to an evaluation method associated with the dynamic effects of pipe whip. In addition, it does make reference to Section 3.6.2.4.1 of the EDCD relating to the protection of equipment in relation to pipe whip, which provides exactly the same information as that stated within Section 16.5.1.4 and therefore, does not provide any link to specific claims made related to postulated pipe failure.

348 TQ-AP1000-1288 was raised seeking further information relating to the Pipe Rupture Hazard Analysis (PRHA) that has been undertaken on the AP1000. The response provided an overview of the detailed pipe rupture analysis undertaken of the AP1000 design and included consideration of:

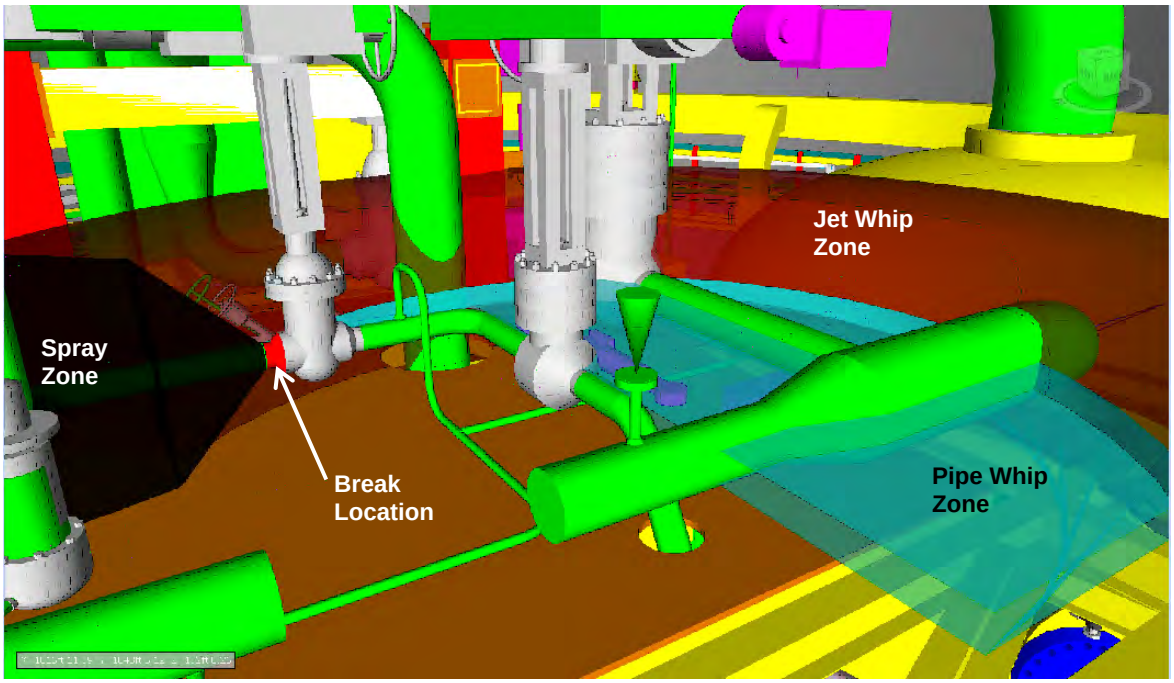
- High-energy and moderate-energy system / line identification

- Integration with Break Exclusion Zone (BEZ) and Leak-Before-Break (LBB) boundaries
- Postulated break locations
- Dynamic effects including:
  i) Pipe whip and jet impingement loads on structures
  ii) Unrestrained and Restrained Zones-Of-Influence (ZOIs) in 3D plant model
  iii) Sub-compartment pressures
- Flooding levels and hydrostatic loads on walls
- Identification of accident mitigation / safe shutdown SSCs in ZOIs
- Environmental effects of sprays and drips on equipment
- Operability assessment (accident mitigation / safe shutdown capability)
- Whip restraints / jet shields / Restrained ZOI

349 From the analysis undertaken for potential break locations, the analysis considers what plant and equipment requires protection against such events and can include pipe whip restraints, barriers and shields, as well as specific protection to SSCs against the environmental effects of a postulated pipe rupture.

350 Figure 2 presents part of the analysis undertaken for a break in the Reactor Coolant System. The red segment at the valve is the break, the black cone is the spray zone, blue curve is the pipe whip zone, and the large red arc is the jet whip zone.

Figure 2 – Pipe Rupture Analysis Screenshot from the 3D Model



351 As can be noted from the screenshot within Figure 2, the analysis considers many factors associated with pipe breaks including potential hinge effects, the consideration of jet impingement and spray effects on safety significant SSCs.

352 The response to TQ-AP1000-1288 identified that the work undertaken as part of the PRHA is ongoing and the intention of the complete analysis is to demonstrate that the plant can be safely shutdown and maintained in a safe shutdown condition following each postulated pipe rupture. However, some pre-emptive evaluation work has been undertaken in order to provide confidence that the AP1000 design would accommodate the effects of pressure part failure. The evaluation:

- Ensured that potential pipe whip restraints could be spatially accommodated by the plant design,
- performed bounding studies on affected structures, regarding their integrity to accommodate associated pipe whip effects, and;
- affected designs of structures to ensure sufficient venting areas for effects of sub-compartment pressurization for potentially problematic areas.

353 In addition, TQ-AP1000-1288, confirmed a schedule for the remaining work to be undertaken as part of the PRHA.

354 I am satisfied that the approach taken to the analysis of potential breaks is robust and rigorous. The potential consequences of pipe failures associated with all potential break locations and the consideration of the protection that is required for each of the locations is in line with my expectations. As was mentioned previously the locations for pipe whip restraints have been identified and are captured within the PCSR, however, there is uncertainty associated with claims made on barriers and / or shields to mitigate against potential pipe ruptures.

355 In addition to the PRHA, there was also a need to seek further detail on the proposed changes to be made to the PCSR associated with pressure part failure post GDA. The response to TQ-AP1000-1272 included the following amendment:

Change made	Reason for change	Effect on Claim, Argument or Evidence
Additional detail added from PPF analysis to identify the areas for which high energy pipe rupture have been assessed.	High energy pipe rupture identified in accordance with the pipe rupture design criteria is limited to SSCs within the CVS within Rooms 12156 and 12255. This was not brought out in Rev A of the PCSR.	Clarification to argument. Reference 11.53

356 This change is associated with the outcome of the analysis outside of Containment and identifies that there is only one system located within two rooms of the Radiologically Controlled Area (RCA) of the Auxiliary Building. I am content that the CVS is the only system identified through the pipe rupture analysis that required consideration given the criterion laid down within the pipe rupture analysis. It should be noted that the analysis does not include the MSIV Compartments as, due to the application of claims made relating to break exclusion areas, the areas fall outside the scope of the PRHA. The assessment of the MSIV Compartments is addressed specifically within the following section of this assessment report.

357 A further change to the PCSR within this area that Westinghouse have identified is associated with the need to provide a definitive list of all barriers, shields and pipe whip

restraints as part of the safety case for pressure part failure. The response to TQ-AP1000-1272 includes the following:

Change made	Reason for change	Effect on Claim, Argument or Evidence
Statements included providing clarity on the current development of the PPF analysis and interaction with the final AP1000 design.	In reviewing supporting information to determine which barriers need to be claimed as providing protection against pipe whip following a PPF it was clear that the PPF analysis needed to be re-visited when the final pipe work design was being completed.	Does not modify the claim but recognises that full and definitive list of claims on all barriers, shields and pipe restraints will not be available until final design stage.

358 Given the need to identify the definitive claims made on barriers, shields and pipe restraints, a GDA Issue has been identified within this area (**GI-AP1000-IH-03**) relating to the safety case for Pressure Part Failure which has an associated GDA Issue Action (**GI-AP1000-IH-03.A1**) requiring the detailed claims and arguments associated with the engineered provisions in place to protect against potential pipe breaks. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

359 Further to the identified inconsistency associated with claims made upon pipe whip restraints, barriers and shields, I decided to sample into the provisions in place against the effects of failure of either the main steam line or main feedwater line within the Main Steam Isolation Valve (MSIV) Compartments

360 The MSIV compartments (rooms 12404 and 12406) in the clean Auxiliary Building house the main and start-up feedwater lines and feed and main steam lines. PCSR Section 11.6.4.2 states:

"*The auxiliary building contains radiologically controlled and non-radiologically controlled (clean) areas that are physically separated by structural walls and floor slabs. These structural barriers, and the associated penetrations, are designed to prevent the effects of postulated pressure part failures within one part of the building from damaging Class 1 SSCs contained within the other half. Further details are provided in the AP1000 Barrier Matrix [Ref. 11.7].*"

361 Furthermore, PCSR Section 11.6.4.2 states:

"The hazard barrier matrix [Ref. 11.7] demonstrates that the walls of the MSIV compartments are sufficiently robust that an impact arising from pipe whip of a main steam or feed line would not result in damage to SSCs delivering safety functions elsewhere in the auxiliary building. In addition, the compartment walls will also prevent the spread of steam or water from steam releases or water spray incidents from affecting the remainder of the clean auxiliary building (see the AP1000 Barrier Matrix [Ref. 11.7] for further details)."

362 As part of my assessment I reviewed the AP1000 Barrier Matrix with the intention of assessing the arguments and evidence. The AP1000 Barrier Matrix identified the wall and floors of the MSIV compartments having a 3 hours fire barrier resistance and 6 psi design pressure withstand capability. However, it did not provide demonstration that the walls of the MSIV compartments are sufficiently robust that an impact arising from pipe whip of a main steam or feed line would not result in damage to SSCs delivering safety functions elsewhere in the auxiliary building.

363 As mentioned previously, relating to barriers and shields, Section 16.7.6 of the PCSR refers to Section 3.6.2.4.1 of the EDCD which states that barriers and shields are provided against the effects of jet impingement. Section 3.6.2.4.1 of the EDCD then refers to Sections 3.8.3 and 3.8.4 of the EDCD for design criteria and loading combinations. However, Section 3.8.4.3.1.4 of the EDCD then refers back to Section 3.6 of the EDCD.

364 Therefore, as was the case with the assessment undertaken on the principal claims, arguments and evidence, the PCSR in this area is not clear and there are a number of circular references which ultimately result in a lack detailed arguments or evidence being presented on the ability of the MSIV structure, including pipe whip restraints, barriers or shields, to withstand pipe whip and / or jet impingement loads.

365 To conclude, I am uncertain of the specific claims, arguments and evidence associated with pipe break within the MSIV Compartments as Chapters 11 and 16 of the PCSR, the AP1000 Barrier Matrix and the EDCD do not identify the specific claims made on the provisions in place to protect against failure of the Main Steam and Feed Water Lines within these areas.

366 This shortfall has been identified by Westinghouse and the response to TQ-AP1000-1272 identifies changes to the PCSR as a result of further pressure part failure analysis undertaken within the MSIV Compartments:

Change made	Reason for change	Effect on Claim, Argument or Evidence
Additional detail added from PPF analysis to state that no high energy break locations were identified in the clean auxiliary building based on application of the pipe rupture design criteria. This includes the MSIV compartments (12404, 12504, 12406, 12506). Main steam and feed pipe work in MSIV rooms is within a break exclusion zone. However a break assessment has been carried out to determine the requirement for pipe work restraints. Statement that Barrier Matrix demonstrates robustness of MSIV compartment walls has been removed and replaced with statement that the Barrier Matrix provides summary of the requirements placed on barriers. The MSIV room walls are now claimed as a defence in depth measure.	Section 11.6.4.2 in Rev A of PCSR made a claim on the walls of the MSIV compartments to resist pipe whip of the main steam or main feed lines. During updating of the Barrier Matrix to Rev B the claims made against walls and floors were re-investigated, including those resulting from PPF. These confirmed that the approach taken when addressing the hazards related to failure of the main steam or main feed lines in the MSIV compartments has been to apply design codes to ensure that the pipe work can be claimed not to exhibit double ended rupture. Hence, this pipe work is located in a break exclusion zone. A longitudinal crack is still assumed so that the location and design of pipe whip restraints can be determined. These are designed to prevent a pipe impacting the MSIV compartment walls, floor and ceiling. In addition, the environmental effects are evaluated. The MSIV/MCR wall is a structure that is designed to withstand the pressure, spray and jet effects of a pipe break. Its ability to withstand a pipe whip incident has not been assessed as pipe whip events are prevented by application of break exclusion criteria and use of pipe whip restraints. The MSIV/MCR wall is however a substantial concrete wall being 2 foot thick. It is therefore expected to offer protection to the MCR should a pipe whip event occur.	The claim on the pipe whip withstand ability of the MSIV to MCR wall has been removed as it is unnecessary. The claim has been replaced by one which is made up of two parts. • A claim that the pipe work will not break as it complies with the requirements for inclusion in a break exclusion zone. • A defence-in-depth argument that the pipe work restraints will prevent the pipe work impacting the MSIV compartment walls. Therefore, the MSIV/MCR robust wall structure is now identified as a defence in depth measure.

367 As this change has not been subject to assessment during Step 4, a GDA Issue Action (**GI-AP1000-IH-03.A2**) requiring Westinghouse to provide the revised safety case for the MSIV Compartments. This action is part of the broader GDA Issue relating to the safety case for Pressure Part Failure (**GI-AP1000-IH-03**) (see Annex 2).

4.5.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

368 The SAPs, state within SAP EHA.5 and SAP EHA.6:

Engineering principles: external and internal hazards	Operating conditions	EHA.5
Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.		

Engineering principles: external and internal hazards	Analysis	EHA.6
Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.		

369 This is further reinforced by SAP EHA.14:

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

370 NS-G-1.11 states within paragraph 3.55:

"The whipping pipe branches should be analysed geometrically to determine possible directions of motion that might endanger target SSCs, as well as to evaluate their kinetic energy. Any possible mechanical impact on the target should be investigated by means of an appropriate dynamic analysis made on the basis of a detailed assessment of the system transient, to quantify the discharge forces and the energy of the whipping pipe as well as the fraction of the energy that would be transferred to the target (the extent of the analysis can be limited on the basis of conservative assumptions). In addition, the analysis should include an assessment of the effectiveness of the pipe whip restraints, demonstrating that pipe deflections may be kept small by the physical restraints. In the case of terminal end breaks, consideration should be given to the secondary effects on the remaining terminal ends."

371 The SAPs and IAEA guidance quoted above, consider that detailed analysis of failures associated with pipe breaks be analysed quantitatively to determine their potential impact on adjacent safety significant SSCs and to determine the extent of protection required to ensure that postulated failure does not result in a detrimental effect on nuclear safety.

4.5.4 Conclusions of the Pressure Part Failure Assessment

372 My assessment has identified a somewhat confusing and contradictory approach to the construction of the safety case for pressure part failure with a number of circular references made to the source of the claims, arguments and evidence. The PCSR and supporting references do not make it clear what provisions are in place to protect against the effects of pressure part failure. This may be in part due to the incomplete pipe rupture analysis which has yet to adequately inform the safety case in this area. Notwithstanding this, the assessment of the information provided associated with the pipe

rupture analysis currently being undertaken, provides a great deal of confidence that the potential pressure part failures will be captured and marshalled accordingly. Given that this information was incomplete at the time of writing this report and that the impact of the analysis may result in changes to the design of AP1000 in relation to pipework and civil structures, the GDA Issue Action (**GI-AP1000-IH-03.A1**) is warranted.

373 The inconsistent approach to the safety case for the MSIV Compartments highlights shortfalls in the consistency and robustness of the claims made given that there is uncertainty within the PCSR itself and the reference documentation as to exactly what the fundamental claims are within this area. Westinghouse has identified this shortfall and intends to address it within the next revision of the PCSR. Given that the location of the MSIV Compartments it is essential that the case within this area is explicit and involves claims and arguments that can be supported by the detailed supporting evidence. A GDA Issue Action (**GI-AP1000-IH-03.A2**) has been raised requesting the revised PCSR given the significance of the concern.

374 The following GDA Issue has been identified and contains two GDA Issue Actions:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Structural Integrity		
GDA Issue Reference	**GI-AP1000-IH-03**	**GDA Issue Action Reference**	**GI-AP1000-IH-03.A1**
GDA Issue	Provide substantiation to support claims and arguments made within the area of pressure part failure.		
GDA Issue Action	Identify and substantiate all nuclear significant pipe whip restraints, barriers and shields claimed for the protection of redundant trains against the effects of pressure part failure. This substantiation should take consideration of the following: • Quantitative assessment of the consequences of postulated pipe failures (including high energy pipework that is not claimed as HSS derived from the pipe rupture analysis. • Justification of the method applied to selection of the type of protection adopted e.g. pipe restraint, barrier or shield. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Structural Integrity		
GDA Issue Reference	**GI-AP1000-IH-03**	**GDA Issue Action Reference**	**GI-AP1000-IH-03.A2**
GDA Issue Action	Provide the updated safety case that details the identification and substantiation of all claims made in relation to Main Steam Isolation Compartments associated with pressure part failure. This substantiation should take consideration of the following: • Structural integrity claims made on the main steam line and feedwater line pipework. • Engineered design provisions in place to either prevent or mitigate the potential consequences of pipe failure within the two MSIV Compartments e.g. pressure relief paths, valve actuation etc. • Whether there is a requirement for passive features such as pipewhip restraints, barriers or shields. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

4.6 Nuclear Directorate Assessment of Internal Explosion

375 The PCSR at Step 3 (Ref. 18) identified two sources of potential explosions; the first arising from the combustion of flammable liquids or gases, and the second source associated with hydrogen explosion. Potential explosions arising from the combustion of flammable liquids and gases are associated with sources outside the nuclear island. The only sources of explosion within the nuclear island are attributable to the hydrogen supply line, to hydrogen generation associated with reactor chemistry, and to hydrogen accumulation within battery rooms.

4.6.1 Scope of Assessment Carried Out

376 The assessment has focused on the arguments and evidence associated with the claims made within the PCSR associated with the five Class 1 battery rooms in the clean auxiliary building, and with the hydrogen supply system to CVS.

377 Potential explosions from combustion of flammable liquids or gases have not been considered in this assessment as their location; geometry and extent are considered to be Phase 2 licensing matters. Hydrogen generation associated with the reactor chemistry has been considered as part of the AP1000 Step 4 Reactor Chemistry Assessment (Ref. 45).

4.6.2 Assessment

378 Section 11.7.3 of the PCSR states that "*The potential for internal explosions to cause significant damage to SSCs is minimised by limiting and controlling explosive gas inventory of the plant, and by design, construction, operation and maintenance of components containing potentially explosive material and by segregating SSCs from areas containing explosive materials.*"

379 In order to verify the above claim, I particularly focused on the arguments and evidence relevant to the five Class 1 battery rooms in the clean auxiliary building and also to the supply of hydrogen to CVS within containment.

4.6.2.1 Class 1 Battery Rooms

380 Section 11.4 of the PCSR, relating to internal fire, states that due to the electrical isolation and physical separation prevent a hydrogen explosion causing loss of more than one division. It then states that hydrogen issues are discussed further in Section 11.7.

381 During Step 4, Westinghouse undertook a review and comparison of US codes and standards with UK standards and it was identified that the Institute of Electrical and Electronic Engineers (IEEE) standard 484 (Ref. 46), "*Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications*" differed to BS 6133:1995 (Ref. 47), "*Code of Practice for Safe Operation of Lead Acid Stationary Batteries*" in that IEEE 484 recommends maintaining hydrogen concentration levels to be less than 2% whereas BS 6133 calls for concentration levels to be maintained lower than 1%. Westinghouse has changed the design to reflect the need to maintain hydrogen concentrations below 1%.

382 In line with the above modification, the PCSR claims that the mechanical ventilation system is sized so that at the maximum hydrogen generation rate, the hydrogen concentration does not exceed 1%. However, this claim is not supported by analysis demonstrating that the design of the ventilation system ensures that an explosive atmosphere cannot be generated. I would have expected to see calculations detailing the time it takes for the battery rooms to reach 1% hydrogen at worst generation rate during normal and fault conditions.

383 The PCSR states that the battery charges are not interlocked with the exhaust fans or with the flow sensors and, therefore, the chargers do not automatically stop charging if the airflow is stopped. Similarly, the hydrogen detectors in the battery rooms would not automatically cease charging of the batteries. On low flow from the battery rooms the low flow sensors will annunciate an alarm in the MCR to alert the operator to take appropriate action. The AP1000 design, therefore, relies on HVAC procedures which would direct the operators to confirm that battery charging has stopped on loss of ventilation to a battery. The PCSR did not identify any potential fault scenarios leading to partial or complete loss of the ventilation system whilst charging, and the measures in place to prevent a build up of an explosive atmosphere within the battery rooms. However it does state that loss of HVAC would lead to cessation of battery charging but the PCSR does not provide detailed arguments and evidence to substantiate this claim.

384 Section 11.7.6 of the PCSR indicates that there is a claim based on the internal walls being of a robust construction in order to perform their structural functions and achieve their required fire resistance ratings and as a result the walls provide some protection against the effects of internal explosions. However, the safety functional requirements of a 3hr fire barrier are different to the safety functional requirements of a barrier designed to withstand specific explosion overpressures. Therefore, no arguments or evidence have been presented in support of the claim made.

385 The case appears to be primarily associated with the operation of the ventilation extract maintaining the hydrogen concentrations below 1%; however, these systems do not appear to be formally claimed. Rather, the case is presented in a somewhat confusing manner; it states that the ventilation system is sized to ensure that this concentration is

kept below 1% but there is no reference made to potential hydrogen accumulation rates during charging. Furthermore, the case states that the extract system is not interlocked with the battery charging, and the apparent claim made on barriers lacks detailed substantiation.

386 As such it is not clear whether loss of the battery room ventilation systems would lead to an explosive atmosphere during charging. It may be the case that there are detailed arguments and evidence that should power be lost to the fans, charging would cease due to common electrical supplies, and should there be an individual fan failure, due to redundancy in the provision of the fans extract would be maintained. This in addition to hydrogen detection within the battery rooms and the time taken for an explosive atmosphere to be generated in the case of loss of ventilation may be sufficiently long to demonstrate that an adequate case can be made within this area.

387 Due to the lack of clarity within the PCSR, it is not possible to make a judgement associated with the adequacy of the claims made or indeed fully understand the extent of the claims being made in relation to battery room explosion. As a result, a GDA Issue has been raised seeking substantiation of the claims and arguments made within the area of internal explosion (**GI-AP1000-IH-04**) with a specific GDA Issue Action (**GI-AP1000-IH-04.A1**) requesting substantiation of the safety case for explosion within Battery Rooms. The complete GDA Issue and associated actions are formally defined in Annex 2 of this report.

4.6.2.2 Supply of Hydrogen to CVS

388 Hydrogen is supplied to the CVS within the containment by the Plant Gas System (PGS). The supply line passes into the Turbine building wall, through the first bay of the Turbine Building where it passes into Auxiliary Building. The line is routed through rooms 12306, 12341, 11300, 11209, 11204, 11304, 11303 and 11301. The PCSR states that the supply line to CVS does not pass through compartments containing Class 1 and Class 2 equipment or near ignition sources. However, this is inconsistent with Table 9A-2 of EDCD, which lists all Class 1 SSCs for each fire zone. The following fire zones, containing Class 1 SSCs, have the hydrogen supply line to the CVS routed through them.

- Fire Zone 1100 AF 11204 - Room 11204. Includes the Class 1 SSCs for the RCS - hot leg 1 wide range pressure component.
- Fire Zone 1100 AF 11300 A&B - Room 11300. Includes various Class 1 SSCs for the PCS, RCS, VFS, PXS, and SGS, supplied by Division B and D Class 1 essential DC and UPS cables.
- Fire Zone 1100 AF 11301 - Room 11301. Includes various Class 1 SSCs for the RCS and SGS.

389 It should be mentioned here that a fire zone may include a number of rooms. From the information given within the PCSR, the Internal Hazards Topic Report and the EDCD it is difficult to ascertain the exact room location of the above Class 1 SSCs, but it is conservative to assume that an explosion in a fire zone will cause complete loss of the Class 1 SSC in that fire zone.

390 The qualitative analysis provided within the PCSR includes arguments that the compartments through which the line passes are ventilated, and are large enough (>365 m^3) that release of a complete cylinder would not reach the LFL of 4%, however, the PCSR did not explicitly consider all individual rooms where the supply line is routed

through. It is reasonable to assume that, given the limited hydrogen supply, the relatively large volumes and the ventilation systems in place, the potential for an explosive atmosphere to be realised is remote, however, it is not possible to state with confidence that an explosive atmosphere would not occur.

391 The response to TQ-AP1000-1272 identified a number of changes to be made to the next revision of the PCSR. All four claims are to remain unchanged with the only change being to the addition of reference 11.6 that provides detailed information relating to the routing of the hydrogen supply. The following extract from the TQ response provides information relating to the changes to be made:

Change made	Reason for change	Effect on Claim, Argument or Evidence
Clarified that wall thickness is nominally 0.6m.	Clarification to ensure that wall thickness is correctly interpreted.	No effect.
Clarified that "safe distance" is conservative margin of safety.	Clarification to emphasise that there is conservatism in margin of safety.	No effect.
Clarified the structural ability to protect from a credible explosion.	Clarification to reflect that explosions are exterior to the Nuclear Island.	No effect
Add additional reference to end of section. The new reference is 11.6.	New assessment available that supports the PCSR for internal hazards. It provides additional detailed information on routing of hydrogen supply line. See Westinghouse Letter UN REG 000490 and Westinghouse / ND Internal Hazards GDA Step 4 Meeting Level 3 Minutes, 5 January 2011.	Supporting evidence provided.

392 A further TQ (TQ-AP1000-1286) was raised seeking the specific changes that were to be made to the PCSR including the supporting justification to the changes associated with the claims, arguments and evidence presented within the PCSR. The response states:

"Relative to the Internal Explosions safety case changes, revision 0 of the PCSR reflects additional emphasis minimising the potential for an explosion through control of explosive sources. This emphasis reflects both the minimal use of potentially explosive material in the NI and a qualitative consequential explosive impact relative to the safety of the AP1000.

As an example of the latter, a hydrogen explosion in one or more of the five Class 1 battery rooms does not affect the ability of the AP1000 to safety shut the plant down and maintain the plant in a safe mode since the batteries are designed for use only under loss of ac power scenarios. Given that hydrogen is generated only under charging conditions (i.e., when ac power is available and the batteries are charging), a hydrogen explosion when the batteries are discharging is an extremely low probability event. Upon loss of single battery bank, through explosive means or otherwise, the plant is directed to shutdown. Such an action does not require the batteries.

Further arguments are provided relative to the normally operating containment HVAC in dispersing any evolved hydrogen (from any source) into the containment atmosphere as insufficient to increase the hydrogen concentration significantly. The containment

atmosphere hydrogen concentration is continuously monitored and alarmed in the MCR and the containment is equipped with passive autocatalytic hydrogen recombiners that limit the hydrogen concentration to well below the LFL.

Additionally, the PCSR, revision 0, has minimised the claim that civil structures are required to contain explosive influences within the NI. With a minimisation of explosive potential and segregation of Class 1 SSCs, reliance on civil structures to contain internal explosions is consequently reduced. Note that explosions external to the NI will necessarily retain the same use of civil hazard barriers."

393 In addition, Westinghouse has confirmed that, *"Cross referencing the Internal Missile safety case to the EDCD, Internal Hazards Topic Report, other sections of the PCSR including Internal Missiles, Pressure Part Failure, and Dropped Loads safety cases has been reviewed and incorporated within revision 0 of the PCSR."*

394 Furthermore, Westinghouse confirmed that they have identified a number of limitations in Revision A of the PCSR, which they believe are primarily associated with differences between the UK and US regulatory approaches and state that such differences will be addressed in a future issue of the PCSR. Westinghouse believes that, from an internal hazards perspective, the overall robustness of the AP1000 design means that minimal design and supporting analysis changes have resulted from this work. However, Westinghouse recognises that there may be a need for GDA Issues within this area which may lead to a requirement to provide further substantiation.

395 Given that the revised PCSR has not yet been issued and given the concerns identified within my assessment, a specific GDA Issue Action (**GI-AP1000-IH-04.A2**) has been raised requiring substantiation of the safety case for the routing of hydrogen supply pipework of the CVS within areas containing Class 1 SSCs. This Issue Action is contained within the broader GDA Issue (**GI-AP1000-IH-04**) (see Annex 2) associated with hydrogen explosion.

4.6.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

396 The SAPs state in SAP EHA.14:

Engineering principles: external and internal hazards	**Fire, explosion, missiles, toxic gases etc – sources of harm**	**EHA.14**
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

397 The ND TAG, T/AST/014 provides further information relating to the need to assess facilities against the potential effects of internal explosions. Section 5.8 of the guidance states:

"Consideration should be given to a need for redundancy and segregation in the design and layout of items important to safety to mitigate against any potential threat from explosions and missiles. The hazards should be prevented or minimised but where they are not avoidable items important to safety should be protected by spatial or physical barriers."

398 Included within the TAG are specific matters that should be addressed in the design and safety of the plant, which include:

- Sources of possible explosions/missiles should be identified, the possible magnitude of explosions, blast waves and the likely size, frequency and trajectory of missiles estimated, and their effects on items important to safety assessed.
- The results of a hazard analysis in conjunction with the licensee's acceptance criteria should be used to verify the adequacy of protection provided by spatial segregation, protective barriers, and redundancy in safety related items and safety systems.
- Possible causes of explosions to be considered include the ignition of flammable gas, vapour or oil-mist clouds, exothermic reactions, pyrophoric materials, failure of pressure parts, and explosions associated with switchgear, high energy transformers, electrical batteries, terminal boxes and power cables.
- Hydrogen must be treated with particular care as hydrogen explosions can be very violent. Flammable and potentially explosive gases such as propane and butane are burned to supply heat for carbon dioxide and nitrogen vaporisation. In addition to the effects of blast overpressure, the hazard analysis should consider the heat and toxicity of hot or burning gases, fire, and the generation of missiles.

399 In relation to the potential for a explosive atmosphere within battery rooms associated with the production of hydrogen from the batteries during charging, BS6133:1995, *"Code of Practice: Safe operation of lead-acid stationary batteries"* states:

"*The volume of hydrogen obtained can be expressed as a percentage of the total volume of the room or cabinet/cubicle, and this can be used to calculate the number of air changes per hour necessary to keep the hydrogen concentration below the recommended maximum of 1 % (V/V).*"

400 The PCSR did identify sources that could give rise to an explosion but did not quantitatively specify their consequences, and did not identify the systems in place to prevent, protect or mitigate their consequences.

4.6.4 Conclusions of the Internal Explosion Assessment

401 The analysis presented within the PCSR identified potential sources of explosions but failed to quantitatively present a multi-legged argument associated with the systems in place to prevent, protect and mitigate the potential consequences. Westinghouse has identified a number of limitations in Revision A of the PCSR, which they believe are primarily associated with differences between the UK and US regulatory approaches. They believe that, from an internal hazards perspective, the overall robustness of the AP1000 design means that minimal design and supporting analysis changes have resulted from this work. However, Westinghouse recognises that there may be a need for GDA Issues within this area which may lead to a requirement to provide further substantiation.

402 The following GDA Issue has been raised associated with internal explosion and includes two GDA Issue Actions:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-04**	**GDA Issue Action Reference**	**GI-AP1000-IH-04.A1**
GDA Issue	Provide substantiation to support claims and arguments made within the area of internal explosion.		
GDA Issue Action	Provide substantiation of the safety case for explosion within Battery Rooms. This should include consideration of a multi-legged argument associated with the following: • Potential hydrogen accumulation rates during normal and fault conditions. • Consideration of heating, ventilation, and air conditioning (HVAC) systems. • Hydrogen detection. • Engineered protection systems associated with the cessation of battery charging. • Civil structures in place to prevent propagation of a hydrogen explosion to redundant trains of protection. Administrative controls or procedures presented as risk mitigation. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-04**	**GDA Issue Action Reference**	**GI-AP1000-IH-04.A2**
GDA Issue Action	Provide substantiation of the safety case for the routing of the hydrogen pipework within areas containing Class 1 SSCs. This should include consideration of a multi-legged argument associated with the following: • Potential hydrogen accumulation rates during normal and fault conditions. • Consideration of heating, ventilation, and air conditioning (HVAC) systems. • Hydrogen detection. • Civil structures in place to prevent propagation of a hydrogen explosion to redundant trains of protection. • Administrative controls or procedures presented as risk mitigation. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

4.7 Nuclear Directorate Assessment of Internal Missiles

403 The PCSR at Step 3 (Ref. 18) provided high level principle based statements relevant to failure mechanisms resulting in missiles generation and on the prevention of missile impact on safety significant SSCs. These were assessed in the Step 3 Assessment Report and found that there was a shortfall in the provision of the claims and arguments.

404 The Step 3 Assessment Report also assessed the statements made in the EDCD and concluded that although the methodology applied to the design of the AP1000 in relation to missile impact is consistent with that stated within the TAG, T/AST/014, there are a number of non specific principle based claims with no supporting arguments. In addition, it was unclear what plant is claimed, and there was no substantiation of the SSCs provided. Furthermore, consequential effects of hazards such as dropped load induced missiles were dismissed with no substantiation provided detailing why missiles generated as a result of such an event was incredible.

405 The approach to during Step 4 was to undertake assessment of the case for internal missile generation presented in the PCSR with a view to explore the detailed arguments and evidence.

4.7.1 Scope of Assessment Carried Out

406 The assessment has focused on the arguments and evidence required to support the claims made within the PCSR. The approach to the assessment is to consider the claims made and determine whether there are adequate arguments and evidence in place to support those claims.

4.7.2 Assessment

407 The safety design approach described in Section 11.8.2 of the PCSR states that:

"The consequences of missile generation are mitigated through the provision of segregation barriers that can withstand the impact of possible missiles such that the Category A safety functions and post-72-hour Category B safety functions are not compromised. Additionally redundant safety equipment is segregated by distance from the missile source.

The civil engineering structures provide structural support to the SSCs, but also act as suitable barriers for a number of functions including the prevention of accidentally generated missiles from travelling to a location where significant harm could occur. The justification of the civil structure design with respect to the internal missile safety function is presented in Chapter 16 of this PCSR."

408 Chapter 16 of the PCSR was reviewed to determine the basis and examine the evidence in support of the claims that are made within the PCSR section above. Chapter 16 refers back to Chapter 11 of the PCSR and the AP1000 Barrier Matrix for information on the claimed barriers, and did not include any justification for the claims made on the civil structure. Chapter 16 Section 16.1.5.2 states:

"Nuclear safety functions placed on the civil engineering structures are addressed by demonstrating that the civil structures will withstand the loads arising from normal operations, internal hazards, external hazards, and internal plant faults. The structures need to be appropriately constructed and shown not to suffer any significant deterioration through life. The evidence needed to support a nuclear safety function depends on the significance of the safety function with regards to nuclear safety.

The requirements have been identified for the walls and floors forming the rooms contained within the nuclear island to act as barriers against relevant internal hazards. This information has been presented in the form of a barrier matrix [Ref. 16.9]. PCSR chapter 11 identifies claims with respect to the civil engineering structures. The civil

engineering design addresses loads arising from the following internally generated hazards:

- *Blast pressure*
- *Water pressure*
- *Missiles*
- *Pipe rupture"*

409 Table 16.3 of the PCSR presents the loads identified by the EDCD and addressed by the design. These loads were relevant to external hazards such as tornado and hurricane missile loads, with no reference made to internally generated missiles. Therefore, Chapter 16 of the PCSR appeared only to make claims on the external walls.

410 Furthermore, the AP1000 Barrier Matrix also implies that only external walls of these buildings are claimed and that the potential for internal missiles have been precluded by design. It states that:

"The external structures of the containment and auxiliary building of the nuclear island are required to prevent a design basis missile from causing failure of the SSCs necessary for a safe shutdown of the AP1000. These SSCs are located within the nuclear island. Externally generated missiles are discussed in "Further Evaluation of Potential Tornado Missiles on the Nuclear Island" (Ref.4). This guidance has been incorporated into the structural design guides and therefore is included in the design requirements - Civil Structural Design Criteria (Ref.2) – of the external walls of the nuclear island. These barriers are identified in the matrix as providing missile withstand in accordance with the Civil Structural Design Criteria (Ref.2). Formal missile withstand requirements are not placed on structures within the nuclear island as the approach adopted has been to prevent missiles occurring that would challenge the civil structures. This is done by a combination of design requirements placed on components and systems and for selected locations the use of restraints. These restraints are not included in the matrix."

411 In addition, Section 11.8.2 of the PCSR seems to imply that the barriers claimed for fire will also be able to withstand the effects of internally generated missiles and states:

"….It is argued that the failure of equipment within a segregated area due to missiles is bounded by the fire hazard analysis which assumes that all equipment in such an area can be lost."

412 This claim is not appropriate as the design requirements and substantiation of the 3 hour fire barriers (3 hours fire resistance for integrity, insulation and load bearing capacity) will be different to the design specification and substantiation of missile barriers. As such a missile could potentially disable more than one line of protection as the design and specification for a barrier claimed against missile impact could be more challenging than the design requirements for a fire barrier.

413 The response to TQ-AP1000-1272 detailed a number of changes that were to be made to the next revision of the PCSR. The following changes are quite extensive and were identified in the response to the TQ:

Change made	Reason for change	Effect on Claim, Argument or Evidence
The claim on the civil engineering structures being the principal means of protecting the SSCs providing the Cat A and post 72 hour Cat B safety functions has been clarified. This claim is valid for internal missile hazards that are generated externally to the nuclear island. However it does not capture the full safety design approach adopted to address internal missiles. New text has been included in 11.8.2 to set out the safety design approach. This approach is already contained within section 11.8 of the PCSR, Revision A.	The safety design approach adopted for AP1000 missile hazards is not just to provide barriers. Barriers consisting of the containment building and the exterior walls of the auxiliary building provide missile protection. The safety design approach adopted also seeks to minimise the frequency of an internal missile occurring and minimising its potential to disrupt Class 1 SSCs. The approach is: • Application of design codes to minimise the potential for a pressure part failure that could generate a missile. • Incorporation of design features in components to prevent missiles being generated external to the component. • Orientating components, such as the main turbine, to direct any missile away from Class 1 equipment Locating Class 1 SSCs outside the zone of influence of a potential missile where practicable using either distance or separation by a structural barrier.	Greater emphasis has been put on the elements of the safety design approach other than a simple claim on structural missile barriers.
Additional text, most of which has been moved from Section 11.8.1, is included to clarify the claims being made against barriers for turbine missiles. These barriers consist of the containment building and the exterior walls of the auxiliary building.	Text clarifies the claim being made against the barriers and shows this is limited to the containment building and the exterior walls of the auxiliary building.	No new claim. Clarify existing claims.
Changes have been made to ensure correct description of containment building	Clarify text to remove ambiguity.	Clarification.
Text clarified to remove statement that the plant can withstand loss of all equipment within a fire area.	The fire assessment argues that the AP1000 will continue to provide Category A and post 72 hour Category B functions after the loss of all SSCs within a fire zone. The statement within 11.8.3.2 went further to include a full fire area. This is not supported by the fire assessment. This contradiction has been removed and	The claim on the ability of the plant to withstand a loss of equipment after a fire has been made consistent with the fire assessment.

Change made	Reason for change	Effect on Claim, Argument or Evidence
	the argument presented made clearer and consistent with the fire assessment.	
A summary of the PPF assessment has been included instead of the discussion of worst case consequences. Cross references have been added to the PPF assessment.	The text included in the PCSR Rev A did not adequately set out the arguments around pressurised components in relation to the PPF assessments that had been carried out. The change made is designed to address this by directing the reader back to the PPF section.	The argument has been improved and the reader directed to the PPF section.
Rewritten section.	The Redundancy, Separation and Segregation section for Missiles in the PCSR Rev A did not provide a structured argument. It has been replaced by a more detailed summary of the arguments related to Redundancy, Separation and Segregation drawn from statements that occur elsewhere in the internal hazards chapter. This while additional text is included, no new information is included.	Clarification to argument.

414 There appears to be one significant change to the claims made on internal missile, which removes any claims made upon barriers other than those of the external walls.

415 A further TQ (TQ-AP1000-1285) was raised seeking the specific changes that were to be made to the PCSR including the supporting justification to the changes associated with the claims, arguments and evidence presented within the PCSR. The response stated that the changes to the PCSR associated with the internal missile safety case has resulted in the claims being made on civil structures being placed into context relative to a range of fundamental barrier protections. Westinghouse recognises that in substantiation of the internal missile safety case there is a need to make reference to the design basis in the prevention of missiles, segregation of Class 1 SSCs, the inability of low and medium pressure sources to create missiles that could result in unacceptable consequences, the robustness of the Nuclear Island civil structures, turbine orientation, and minimisation of explosive missile generation. The approach Westinghouse proposes is to augment the substantiation through the specific identification of sources of internal missiles that are likely to interact with Class 1 SSCs with the expected result being confirmation of the design suitability for internal missiles.

416 In addition, Westinghouse have confirmed that, *"Cross referencing the Internal Missile safety case to the EDCD, Internal Hazards Topic Report, other sections of the PCSR including Internal Explosions, Pressure Part Failure, and Dropped Loads safety cases has been reviewed and incorporated within revision 0 of the PCSR."*

417 Furthermore, Westinghouse confirmed that they have identified a number of limitations in Revision A of the PCSR, which they believe are primarily associated with differences between the UK and US regulatory approaches and state that such differences will be addressed in a future issue of the PCSR. Westinghouse believes that, from an internal hazards perspective, the overall robustness of the AP1000 design means that minimal design and supporting analysis changes have resulted from this work. However, Westinghouse recognises that there may be a need for GDA Issues within this area which may lead to a requirement to provide further substantiation.

4.7.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

418 The SAPs, state within EHA.14:

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

419 IAEA guidance NS-G-1.11 considers the need for barriers and physical separation to be adopted when there is the potential for missiles to result in loss of redundancy and that such barriers should be sited close to the source of the missiles. Westinghouse claims such barrier within the design but they failed to state, explicitly, the location of the barriers claimed in the safety case, and failed to provide the adequate substantiation.

420 Paragraph 3.27 of NS-G-1.11 states:

"Evaluation of the adequacy of barriers, whether they are structures provided for other purposes or special missile barriers, necessitates the consideration of both local and general effects of missiles on the barrier. Depending upon the postulated missile's mass, velocity and impact area, the local or the general effect of the missile may dominate, but both should be evaluated. Local effects of missiles are penetration, perforation, scabbing or the ejection of concrete blocks and spalling, which are limited mainly to the area of impact on the target. General effects of missiles include buckling or structural failures in bending, tension or shear. Small missiles such as valve stems will have mainly local effects, while large, slow moving missiles such as those arising from structural collapse or falling loads will have mainly general effects."

421 Therefore, IAEA guidance NS-G-1.11 considers the need for barriers and physical separation to be adopted when there is the potential for missiles to result in loss of redundancy and that such barriers should be sited close to the source of the missiles. Westinghouse appears to make claims on barriers within the design but have not explicitly captured the location of the barriers and their substantiation.

4.7.4 Conclusions of the Internal Missile Assessment

422 The PCSR and associated references in the area of internal missile has resulted in a safety case that is confusing and contradictory. Westinghouse has identified a number of limitations in Revision A of the PCSR, which they believe are primarily associated with differences between the UK and US regulatory approaches. They believe that, from an internal hazards perspective, the overall robustness of the AP1000 design means that minimal design and supporting analysis changes have resulted from this work. However,

Westinghouse recognises that there may be a need for GDA Issues within this area which may lead to a requirement to provide further substantiation.

423 Whilst I accept the statements provided by Westinghouse, I am not satisfied that the safety case for internal missiles, as set out within the PCSR, provides an adequate presentation of the claims, arguments and evidence in light of the proposed changes to the PCSR and the need for further work identified within this area. As a result, the following GDA issue has been raised:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-05**	**GDA Issue Action Reference**	**GI-AP1000-IH-05.A1**
GDA Issue	Identify and substantiate the claims, arguments and evidence that constitute the internal missile aspects of the internal hazards safety case.		
GDA Issue Action	Identify and substantiate the claims, arguments and evidence that constitute the internal missile aspects of the internal hazards safety case. This substantiation should take consideration of the following: • Identification of all potential areas where missiles could result in loss of more than one division or train of protection, including failures associated with pressure part failure. • Analysis of the potential consequences associated with internal missile generation. • The identification and substantiation of all engineered prevention features e.g. component integrity, overspeed systems, trip functions etc. claimed for the protection of redundant trains against the effects of internally generated missiles. • The identification and substantiation of all nuclear significant hazard barriers claimed for the protection of redundant trains against the effects of internally generated missiles. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

4.8 Nuclear Directorate Assessment of Dropped Loads and Impact

424 The Step 3 Assessment Report identified concerns associated with the methodology applied in the assessment of dropped load and impact. It was stated within the PCSR that SSCs were justified against collapsing or falling loads through their seismic qualification which demonstrated that they are located a safe distance from potential dropped loads or designed sufficiently to withstand their impact. In addition, the PCSR did not reflect the detailed information, as presented in the EDCD, chapter 9.1.5, relating to the criteria associated with the design and use of lifting equipment within the AP1000 design.

425 During Step 4 I have carried out further assessment of the approach to dropped loads and impact. I focused on the analysis of dropped loads and impacts, as well as of the evidence available to demonstrate that the safety case for potential dropped loads and impacts was robust.

4.8.1 Scope of Assessment Carried Out

426 My assessment of dropped loads and impact involved a detailed review of the basis of the claims, arguments and evidence presented within the PCSR utilising international and UK relevant good practice, for both nuclear generation and nuclear chemical plant facilities. The involvement of other assessors in support of this assessment was required; specifically, mechanical engineering as there were claims made on the lifting equipment itself and claims on the preclusion of dropped loads by design.

4.8.2 Assessment

427 The PCSR claims that the consequences of dropped load are minimised through application of best practice to the design and operation of the cranes complimented with procedural controls:

- Be single failure proof (5 of the 16 lifting devices).
- Be fail-safe on loss of motive power.
- Be fail-safe in the event of a design basis seismic event.
- Have crane controls that allow precise positioning of loads.
- Have monitoring and protection devices to mitigate the risk of a dropped load, overload or crane collapse.
- Have safe load paths specified.
- Have procedural controls linked to plant operating mode to reduce the consequences of a dropped load.
- Have physical stops to prevent the hook from travelling over or near SSCs.

428 The PCSR claims that safe loads paths have been specified in areas where the floors or walls could not withstand the potential dropped load without loss of function or disruption to other SSCs. The AP1000 Step 4 Mechanical Engineering Assessment (Ref. 48) has identified this aspect as an Assessment Finding (AF-AP1000-ME.23) and requires the need for load paths to be determined for all lifts of nuclear safety significance.

429 There is a statement made within the PCSR that relates to claims made on civil structures which identifies that the substantiation of such civil structures is yet to be carried out. Section 11.10.4 of the PCSR states:

"Floors and walls that could be impacted by a dropped load are required to withstand the potential dropped load without loss of function or disruption to other SSCs where failure could lead to the loss of a Category A safety function. If this is not possible, then load paths have been specified to ensure that a dropped load over a Category A safety function will not occur. The substantiation of the floor and wall structures for dropped loads is still to be carried out."

430 As this substantiation has yet to be undertaken and floors and wall structures are not identified, the current PCSR is unclear on the extent of claims made on such structures. Indeed, it may be possible to provide substantiation of dropped loads and impact through other preventative means including engineered protection systems, detailed load paths, localised protection etc.

431 The response to TQ-AP1000-1272 detailed that the section within the PCSR relating to the general substantiation of the floor and structures was to be removed and replaced

with a reference to the EDCD on heavy loads. The basis for this change was stated within the response:

Change made	Reason for change	Effect on Claim, Argument or Evidence
Removed statement that a general substantiation of the floor and wall structures was contained in the PCSR Chapter 16 and noted reference to heavy loads in Reference 11.4.	PCSR Chapter 16 does not provide that level of justification for dropped loads as highlighted in a Level 3 meeting. Reference 11.4 noted as providing additional information on the management of heavy loads.	Greater clarity related to use of civil structures evidence.

432 I have assessed Section 9.1.5 of the EDCD in relation to dropped loads and impact and within Section 9.1.5.3 associated with the safety evaluation it states:

"The polar crane, the cask handling crane, the containment equipment hatch, and the maintenance hatch hoists are single failure proof. These systems stop and hold a critical load following the credible failure of a single component. A double design factor is provided for hooks where used as load bearing components. Redundancy is provided for load bearing components other than hooks, such as the hoisting ropes, sheaves, equalizer assembly, and holding brakes. These systems are designed to support a critical load during and after a safe shutdown earthquake. The seismic Category I equipment and maintenance hatch hoist systems are designed to remain operational following a safe shutdown earthquake. The polar crane is designed to withstand rapid pressurization of the containment during a design basis loss of coolant accident or main steam line break, without collapsing.

The cask loading pit is separated from the spent fuel pool. The cask handling crane cannot move over the spent fuel pool because the crane rails do not extend over the pool. Mechanical stops prevent the cask handling crane from going beyond the ends of the rails.

A heavy loads analysis is performed to evaluate postulated load drops from heavy load handling systems located in safety-related areas of the plant, specifically the nuclear island. No evaluations are required for critical loads handled by the containment polar crane, the cask handling crane, the containment equipment hatch hoist, and the containment maintenance hatch hoist since a load drop is unlikely."

433 This appears to claim that the potential for a dropped load arising from failure of a single failure proof crane is not credible based upon the design of the crane and not upon civil structures. Whilst it is accepted that the crane will be designed and constructed to a high specification, I would still expect to see a consequence analysis undertaken associated with dropped loads and impact.

434 A further TQ (TQ-AP1000-1284) was raised seeking the specific changes that were to be made to the PCSR including the supporting justification to the changes associated with the claims, arguments and evidence presented within the PCSR. The response stated that no significant changes were to be made to Revision A of the PCSR other than the removal of the statement relating to the general substantiation of floor and wall structures being located within Chapter 16 of the PCSR.

435 In addition, Westinghouse has confirmed that, *"Cross referencing the Dropped Loads safety case to the EDCD, Internal Hazards Topic Report, other sections of the PCSR has been reviewed and incorporated within revision 0 of the PCSR."*

436 Furthermore, Westinghouse confirmed that they have identified a number of limitations in Revision A of the PCSR, which they believe are primarily associated with differences between the UK and US regulatory approaches and state that such differences will be addressed in a future issue of the PCSR. Westinghouse believe that, from an internal hazards perspective, the overall robustness of the AP1000 design means that minimal design and supporting analysis changes have resulted from this work. However, Westinghouse recognises that there may be a need for GDA Issues within this area which may lead to a requirement to provide further substantiation.

437 Advice was sought from the Mechanical Engineering Nuclear Topic Group, an internal group comprising of all ND mechanical engineering technical specialists, who have considerable experience relating to lifting equipment and of dropped loads and impact. Their advice was sought in order to inform this assessment of the current approach to dropped loads and impact from high integrity lifting equipment from both a UK and International Standard approach, but also based upon many years experience and understanding of the relevant good practice observed within the UK and overseas.

438 The Mechanical Engineering Nuclear Topic Group advice, following group discussion, was summarised by the following two statements:

- *"Crane and lifting equipment reliability is determined by many factors in addition to equipment integrity. Regardless of integrity claims it is considered necessary to assess the consequences of dropped loads and other malfunctions.*
- *The operating limits and conditions for cranes and lifting equipment should be determined taking account of the failure consequences assessment, and industry and regulatory guidance and engineering good practice, and operation should be demonstrated to be ALARP."*

439 Given that the lack of a supporting consequence analysis for dropped loads and impact, a GDA Issue (**GI-AP1000.IH.06**) (see Annex 2) relating to the need to provide substantiation to support claims and arguments made within the area of dropped load and impact has been raised. The GDA Issue Action (**GI-AP1000-IH-06.A1**) requires the identification and substantiation for dropped load or impact. This approach should, in the first instance, consider the potential consequences on a quantitative basis to determine significance of the dropped load or impact. This should then lead to detailed multi-legged arguments to demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact was ALARP and that such analysis may take into account:

- Claims on civil structures
- Additional physical protection
- Limits and conditions on the use of the lifting equipment
- Provision of detailed load path routes avoiding areas of highest nuclear significance
- Measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised.

440 I have undertaken further detailed assessment on the following two lifting systems given their safety classification and the potential consequences associated with dropped loads and impact:

- The Polar Crane within Containment.
- The Cask Handling Crane within the Spent Fuel Pool area.

4.8.2.1 Polar Crane

441 The Polar Crane is provided in the containment building for lifting and moving heavy loads when the reactor is shutdown (cold shutdown) or during refuelling. In both cases the RCS is below 93^{o}C and its operating pressure is very low or at atmospheric pressure. The crane is designed as a single failure proof crane as specified in NUREG-0554 (Ref. 49) supplemented by ASME NOG-1:1998 (Ref. 50). It is also classed as seismic Category I. A dropped or mishandled load by the Polar Crane has the potential to impact on the component parts of the reactor vessel, integrated head package, the SGs and main steam piping, and the ADS/ Pressuriser. Irradiated fuel or Class 1 SSCs could be damaged. Additionally, the operating floor structure and refuelling cavity floor can be impacted.

442 The dropping of the integrated head package onto the reactor vessel would also impose a large loading onto the reactor pressure vessel with the possibility of damage to the vessel, connecting pipework and supports. The PCSR states that no specific assessment of the AP1000 has been undertaken, but an assessment of the Indian Point 2 and 3 plants, which is quoted as being similar to the AP1000 plant, has shown some damage to the supporting concrete structures. It is not stated within the PCSR whether such an impact could damage Class 1 SSCs or Class 2 SSCs and it is unclear the extent of the damage could be and whether it would have an impact on nuclear safety. This concern is captured through the GDA Issue (**GI-AP1000-IH-06**) (see Annex 2) relating to the substantiation of the dropped loads and impact safety case.

4.8.2.2 Cask Handling Crane

443 The Cask Handling Crane within the radiological auxiliary building lifts the spent fuel shipping cask from the cask transporter in the loading bay of the auxiliary building, moves it into the fuel handling area, and places the cask either in the cask washdown pit or in the cask loading pit. It also used to remove and replace the cask lid. The main and auxiliary hoists are designed as single failure proof as specified in NUREG-0554 supplemented by ASME NOG-1:1998. It is also classed as seismic Category I.

444 The PCSR makes a number of claims including the following:

- The “only” threat of nuclear safety arises from a drop of the fuel cask containing irradiated fuel causing damage to the cask and the fuel within, and a release of radioactivity to the environment.
- A drop of the cask onto the radiological auxiliary building structure could result in localised structure failure of floors and walls. However, the drop of the fuel cask does not cause loss of function of the SFP, disruption to the store fuel or damage to other Class 1 SSCs. The Category A safety function to provide decay heat removal is maintained by the Class 1 SSCs.
- The provision of mechanical stops prevent the cask handling crane from going beyond the ends of the rails and hence prevent a drop of a cask or cask lid into the new fuel store, fuel pond or transfer canal.

445 The high level qualitative analysis presented in the PCSR fails to provide any arguments or evidence that the "only" threat to nuclear safety arises from damage to cask and the irradiated fuel within. 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 presently there is a reliance on administrative controls to ensure that the load path / route is clear of the area directly above these heat exchangers. This potential drop load scenario, and its consequence, has not been captured within the PCSR. Similarly, the PCSR does not discuss the potential (if any) of a drop load to cause loss of cooling water supplies leading to loss of function of Spent Fuel Pool. It is not clear what the extent of the damage could be and whether it would have an impact on nuclear safety, however this concern is captured through the GDA Issue (**GI-AP1000-IH-06**) (see Annex 2) relating to the substantiation of the dropped loads and impact safety case.

4.8.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

446 In terms of internationally accepted standards and guidance, operating experience and relevant good practice, it was considered important to provide an overview of the current expectations associated with dropped loads and impact from both a national and international perspective.

447 The HSE Safety Assessment Principles, SAPs, state within EHA.14:

Engineering principles: external and internal Hazards	**Fire, explosion, missiles, toxic gases etc – sources of harm**	**EHA.14**
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

448 NS-G-1.11 states, *"Structures classified as liable to affect SSCs in the event of their collapse should be designed and built so that the probability of their collapsing can be shown to be negligible; otherwise the consequences of their collapse should be evaluated. Similarly, the hazard posed to SSCs by falling objects (cranes and lifted loads) should be evaluated"*. The approach to the analysis of the consequences within NS-G-1.11 is consistent with the approach adopted within the UK currently.

449 The approach currently undertaken within the UK for the analysis of dropped loads associated with the lifting equipment involves the assessment of the consequences of dropped loads on safety significant SSCs which results in the determination of the limits and conditions of operation of the lifting equipment, detailed load paths, and systems and administrative controls in place.

450 In addition to NUREG-0554, the AP1000 is designed to the US NRC issued NUREG-0612 (Ref. 51), which presents an overall philosophy that provide a defence in depth approach for controlling the handling of heavy loads. The focus of NUREG-0612 is on prevention of dropped loads rather than assessment of the consequences and it subsequently requires the following approach to be adopted within existing US Nuclear Power Plant:

- Assure that there is a well designed handling system.
- Provide sufficient operator training, load handling instructions, and equipment inspection to assure reliable operation of the handling system.

- Define safe load travel paths and procedures and operator training to assure to the extent practical that heavy loads are not carried over or near irradiated fuel or safe shutdown equipment.
- Provide mechanical stops or electrical interlocks to prevent movement of heavy loads over irradiated fuel or in proximity to equipment associated with redundant shutdown paths.
- Where mechanical stops or electrical interlocks cannot be provided provide a single-failure-proof crane or perform load drop analyses to demonstrate that unacceptable consequences will not result.

451 Furthermore, in July 2003, US NRC issued NUREG-1774, entitled, "*A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*" (Ref. 52) in which one of the observations made stated, *"… most load drop events were the result of poor program implementation or human performance errors that led to hoist wire rope or below-the-hook failures. All three very heavy load drops were the result of rigging failures, not crane failures. Consequently, there were no very heavy load drop events that could have been prevented had only a single-failure-proof crane been employed in the lift. However, there were load or hook and block assembly drops that could have been prevented with the use of single-failure-proof cranes and lifting devices."*

4.8.4 Conclusions of the Dropped Load and Impact Assessment

452 To conclude, there is a compelling case, as confirmed within current guidance and standards, operating experience and relevant good practice, in support of the need to undertake a detailed quantitative analysis of the potential consequences of a dropped load or impact arising from the use of lifting equipment.

453 The PCSR claims that floors and walls that could be impacted by a dropped load are required to withstand the potential dropped load without loss of function or disruption to other SSCs where failure could lead to the loss of a Category A safety function. As the substantiation has yet to be undertaken for floors and wall structures are not identified, it is unclear of the extent of claims made on such structures. Indeed, it may be possible to provide substantiation of dropped loads and impact through other preventative means including engineered protection systems, detailed load paths, localised protection etc. The following GDA Issue associated with dropped loads and impact, has been raised:

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Mechanical Engineering		
GDA Issue Reference	**GI-AP1000-IH-06**	**GDA Issue Action Reference**	**GI-AP1000-IH-06.A1**
GDA Issue	Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the AP1000 design.		
GDA Issue Action	Identify and substantiate all claims made on SSCs associated against the effects of dropped load and impact. This approach should, in the first instance, consider the potential consequences of a dropped load or impact on a quantitative basis to determine significance of the dropped load or impact. This should then lead to detailed multi-legged arguments to demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact was ALARP and that such analysis may take into account: • Claims on civil structures. • Additional physical protection. • Limits and conditions on the use of the lifting equipment. • Provision of detailed load path routes avoiding areas of highest nuclear significance. • Measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

4.9 Nuclear Directorate Assessment of Electro-Magnetic Interference

454 The Step 3 Assessment Report identified that EMI may be subject to further assessment during Step 4. Although EMI is identified as an internal hazard within the SAPs it is considered more relevant to be subject to considered as part of the electrical assessment. It has therefore been agreed with the electrical engineering assessor that this is to be captured within the Step 4 Electrical Engineering Assessment of the Westinghouse AP1000 (Ref. 53) and as a result there is no further consideration within this report.

4.10 Nuclear Directorate Assessment of Westinghouse Report, "Applicability of the Control of Major Accident Hazards Regulations (COMAH) to AP1000"

455 The need to subject the report, *"Applicability of the Control of Major Accident Hazards Regulations (COMAH) to AP1000"* (Ref. 54) to assessment was identified within the AP1000 Step 3 Internal Hazards Assessment Report. During Step 4, the Internal Hazards Assessment has identified a number of concerns relating to the fundamental claims, arguments and evidence in relation to nuclear safety. Therefore, the need to prioritise assessment accordingly has resulted in no assessment of the above report being undertaken during Step 4. Given that the report does not form a major aspect of the internal hazards safety case and that it is associated with existing non-nuclear regulations, it is believed that the impact of not undertaking assessment on this report as

part of the Internal Hazards Assessment during Step 4 is minimal and no further action is proposed.

4.11 Nuclear Directorate Assessment of Claimed Operator Actions Associated with Internal Hazards

456 The Step 3 Internal Hazards Assessment Report identified the need for further assessment associated with operator actions in the event of internal hazards as there was some uncertainty as to whether such actions were required as part of the deterministic safety case or if these actions were purely in place as a defence in depth or risk mitigation provision.

457 Further to the issue of the Step 3 Internal Hazards Assessment Report and during my Step 4 assessment, TQs have been raised seeking clarification over whether there are indeed any operator actions claimed as part of the deterministic case. There has also been involvement by the Human Factors Assessment and Probabilistic Safety Analysis areas over the potential "claims" being made on operator actions. The outcome of the assessment during Step 4 through confirmation provided by Westinghouse within the PCSR is that there are no operator actions required as part of the deterministic safety case for internal hazards.

458 As there are no deterministic claims being made on operator response in the event of an internal hazard, no further assessment is required within this area and no GDA Issues or Assessment Findings have therefore been raised.

4.12 Nuclear Directorate Assessment of Categorisation and Classification

459 The Step 3 Assessment Report considered the safety categorisation and classification approach to the fire protection design and stated:

"There are some aspects of the fire protection design e.g. fire barriers and their associated doors, fire dampers and penetration seals, that ND would expect to be classed as 'Safety' due to their function to ensure that fire did not spread to affect more than one train of protection. Within the UK nuclear fleet such items are identified as being necessary to ensure nuclear safety and adequate measures are taken to ensure that these SSCs are designed, maintained and controlled to ensure they perform their required safety function. There is a need for SSCs that perform a nuclear safety function to apply rigorous controls over the design, specification, and installation and to demonstrate that the barriers can be adequately maintained, controlled and monitored throughout the station life. In addition, the application of the single failure criterion, where necessary, would need to be taken into account".

460 Due to the differences in the approach to safety categorisation and classification between the US and the UK, Westinghouse produced a comparison document to address the broad concern relating to categorisation and classification.

461 In addition, Westinghouse has also produced a revised Categorisation and Classification Methodology (Ref. 55) document as well as an AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components document (Ref. 56) both of which have been subject to assessment during Step 4.

4.12.1 Westinghouse Categorisation and Classification Methodology Report

462 The AP1000 UK Safety Categorisation and Classification Methodology document specifies the criteria used to classify the AP1000 SSCs important to nuclear safety in terms that are consistent with the UK SAPs. Therefore, the PCSR and supporting documentation should provide adequate evidence to support the claims made therein.

4.12.1.1 Scope of Assessment Carried Out

463 The assessment is focused on the methodology applied in the Safety Categorisation and Classification document.

4.12.1.2 Assessment

464 The Safety Category indicates how important a function is in maintaining nuclear safety:

- Category A – any function that plays a principal role in ensuring nuclear safety.
- Category B – any function that makes a significant contribution to nuclear safety.
- Category C – any other safety function.

465 The Safety Class indicates how significant the SSC is in maintaining the safety function. In accordance with the Safety Assessment Principles for Nuclear Facilities:

- Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.
- Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function is fulfilled.
- Class 3 – any other structure, system or component.

466 The approach aims to define the quality requirements placed on those SSCs during design and manufacture, and through life. The safety class of a given SSC is used to determine which codes and standards are appropriate to the design and manufacture of that SSC.

467 A number of examples of Category A, B and C safety functions were provided. Those which are relevant to internal hazards are given below:

- Category A safety function "*Protecting SSCs from internal/external hazards that would directly and inevitably result in loss of a principal means of fulfilling a Category A safety function*".
- Category B safety function "*Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the Category B safety functions, such as preventing the spread of fire such that the ability to deliver a specific Category B function is lost*."
- Category C safety function "*Functions to monitor for the occurrence of, and alert personnel to take mitigating action following, internal hazards events (e.g. fire, flood)*".

468 The methodology described in the Safety Categorisation and Classification document is in line with my expectations and SAPs guidance. Its application to AP1000 design is considered in Section 4.12.2 below.

4.12.2 Westinghouse Categorisation of AP1000 Systems and Equipment

469 The application of the Safety Categorisation and Classification methodology is presented in AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components (Ref. 56) which states that "*Classification of SSCs is used to identify those SSCs that play an important part in ensuring nuclear safety. This in turn helps to define the quality requirements placed on those SSCs during design and manufacture, and through life*." The report presents the results of applying the UK categorisation and classification process to the AP1000 SSCs mechanical components, electrical components, instrumentation and control systems, and civil structures.

4.12.2.1 Scope of Assessment Carried Out

470 The assessment is focused on the claims and arguments as presented in the PCSR and the associated evidence presented in AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components document.

4.12.2.2 Assessment

471 The AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components lists a number of SSCs with safety functions relevant to internal hazards including the following:

- The containment vessel and auxiliary building structures are listed as Class 1 providing a Category A safety function - "*Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A*".
- Diesel-Generator Building structure is listed as Class 2 providing a Category A safety function - "*Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions*" The report states that the diesel generator building houses mechanical and electrical equipment that supports a Category A function that is important to safety.
- Containment Polar Crane is listed as Class 1 providing Category A safety functions – "*Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating*)" also "*Preventing the release of radioactive material through the boundary of the reactor coolant system*". The report states that the polar crane protects against load drops on the RCS or on any irradiated fuel assemblies, regardless of location in the transfer canal or vessel.
- Combination Fire/Smoke Dampers in the Auxiliary Building and Annex Building of the non-radioactive ventilation system are listed as Class 2 providing Category A safety function, *"Protecting SSCs from internal/external hazards that could result in the loss of a principal means of fulfilling a Category A safety function."*
- CVS Compartment to Sump, PXS A & B Compartment to Sump, CVS Compartment to Sump, PXS A & B Compartment to Sump and PXS & CVS Compartment Drains are listed as Class 1 providing Category A safety function – *"Protecting SSCs from internal/external hazards that would directly and inevitably result in the loss of a principal means of fulfilling a Category A safety function."* To prevent premature flooding of the PXS compartment and the CVS compartment during a design basis

accident, the drain line from each of these compartments to the sump has two check valves in series which prevent reverse flow through the drain.

472 The following discrepancies between the SSCs listed in AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components and the PCSR have been observed:

- The AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components did not identify the nuclear significant hazard barriers as being explicitly claimed in the PCSR. Section 11.4.3.1 of the PCSR states that structural elements protecting Class 1 SSCs provide 3 hours fire resistance for load bearing, integrity and insulation, and are also Class 1 structures and Section 11.3.2 of the PCSR identifies the hazard barriers between fire areas, which provide protection of redundant equipment to the extent practicable, as Class 1 SSCs delivering Category A safety functions.
- Similarly, the containment Polar Crane is listed as Class 1 SSC providing a Category A safety function, however, the PCSR makes no specific claims against this crane.
- CVS Compartment to Sump, PXS A & B Compartment to Sump, CVS Compartment to Sump, PXS A & B Compartment to Sump and PXS & CVS Compartment Drains are listed as Class 1 providing Category A functions.
- Table 6.4-2 of the Safety Categorisation and Classification Methodology document identifies the fire dampers as Class 2 and lists the relevant Class 2 Codes and Standards. Furthermore, PCSR Chapter 23 – Containment and Nuclear Ventilation states that the highest classification of fire dampers is Class 2. It does however state, "*Combination fire and smoke dampers penetrating fire rated compartment walls will be similarly resilient and meet the single-fault criterion these are provided as a minimum for Class 1 fire barriers*."

473 This result of not capturing the extent of Class 1 claims made within the internal hazards area leads to inconsistency between the classification of SSCs in the Safety Categorisation and Classification Methodology and the PCSR, which impacts on the substantiation of the claims, arguments and evidence. An Assessment Finding (**AF-AP1000-IH-05**) has been raised to address the inconsistencies between the PCSR and the AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components requiring the two documents to be subject to review and address gaps and inconsistency between the documents and ensure that they are captured within the site specific PSCR.

4.12.3 Comparison of the Provisions with International Standards and Guidance, Operating Experience, and Relevant Good Practice

474 The HSE SAPs ECS.1 through ECS.4:

Engineering principles: safety classification and standards	**Safety categorisation**	**ECS.1**
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.		

Engineering principles: safety classification and standards	Safety classification of structures, systems and components	ECS.2
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 regard to safety.		

Engineering principles: safety classification and standards	Standards	ECS.3
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.		

Engineering principles: safety classification and standards	Codes and standards	ECS.4
For structures, systems and components that are important to safety, for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied.		

475 IAEA guidance NS-G-1.7 states:

"*As required in para. 5.1 of Ref. [1], "All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability are commensurate with this classification."*

Where the fire containment approach is used, equipment belonging to a safety system is surrounded by fire barriers capable of resisting the total burnout of the contents of the fire compartment. If the failure of the barriers to fulfil their function in the event of a fire could prevent the meeting of the objectives defined in para. 2.1, it may be appropriate to classify the fire barriers as a 'safety related item'.

Where the fire influence approach is used, safety against the spreading of a fire between redundant safety groups is achieved through the limitation of materials, separation by distance, fire shielding or other local passive protection measures, fire extinguishing systems or a combination of these measures. If the failure of the fire detection or extinguishing systems could prevent the meeting of the objectives defined in para. 2.1, it may be appropriate to classify these systems as a 'safety related system' or a 'safety system' depending on the design and layout of the plant."

4.12.4 Conclusions of the Categorisation and Classification Assessment

476 Whilst the methodology and approach to the categorisation and classification of SSCs is in line with my expectations, my assessment of the AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components document revealed a number of inconsistencies between this document and the PCSR (i.e. source of SSC's).

477 The following Assessment Finding has been raised associated with categorisation and classification:

AF-AP1000-IH-05 – *The Licensee shall identify and address any gaps and inconsistency between the internal hazards aspects of the PCSR and the AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components.*

478 This Assessment Finding should be addressed as part of the following procurement and construction generic milestones for assessment findings:

- Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

4.13 Nuclear Directorate Assessment of Regulatory Observation, RO-AP1000-031

479 During Step 3 a Regulatory Observation (RO-AP1000-031) and associated Regulatory Observation Action (ROA) was raised due to the significance associated with the need to provide an adequate safety case for internal hazards. The RO.A31 stated "*As part of the internal hazards safety case there is a need for Westinghouse to demonstrate that all claims made on Structures, Systems and Components in place to prevent an internal hazard occurring and / or prevent escalation of an internal hazard to be identified and the appropriate arguments and evidence provided to demonstrate that the protection against such hazards has been adequately substantiated*."

480 As a result Westinghouse identified the need to produce an Internal Hazards Topic Report (Ref. 15) that addressed internal hazards as a separate technical area whereas previously it had been split across a number of disciplines. As part of this report it was intended that the document would form a key reference to the PCSR and provide the necessary information required. Revision 1 of the Internal Hazards Topic Report (Ref. 15) was formally issued to ND in August 2009, however, these timescales were insufficient to undertake an assessment of the content within Step 3 and as a result assessment of the Internal Hazards Topic Report had been identified as requiring assessment within Step 4 as part of the assessment of the Internal Hazards Topic Report. Revision 2 of the Internal Hazards Topic Report (Ref. 16) was issued to ND in September 2010, which informed the assessment already undertaken within this report.

481 The assessment of RO-AP1000-031 has therefore been considered as part of the overall assessment undertaken during Step 4 of the GDA and has been reported throughout this report.

4.14 Regulatory Issues

482 There have been no Regulatory Issues produced as a result of the GDA Internal Hazards Assessment of AP1000.

4.15 Interface with Other Regulators

483 There has been an interface with inspectors within HSE who specialise in General Fire Precautions, Conventional Safety, and Construction (Design and Management) Regulations as there was a need to consider the layout of the AP1000 relating to means of escape. A workshop was held by ND to provide Westinghouse an overview of our expectations within this area. Further to the workshop, a letter (Ref. 57) was written to Westinghouse providing some high level comments on a sample of the areas within the AP1000 coupled with an offer to provide further assistance within this area.

4.16 Other Health and Safety Legislation

484 As mentioned above, the interface with other HSE specialists in the fields of fire and construction safety included discussion of the Regulatory Reform (Fire Safety) Order 2005 (Ref. 58) and the Construction (Design and Management) Regulations 2007 (Ref. 59).

5 CONCLUSIONS

485 This report presents the findings of the Step 4 Internal Hazards Assessment of the Westinghouse AP1000 reactor.

486 There are a number of areas where the safety case presented for internal hazards contains inaccurate and inconsistent information, as detailed above, which has resulted in the issue of six GDA Issues comprising of a total of nine GDA Issue Actions. Notwithstanding the GDA Issues raised within my assessment, I believe that the AP1000 design is clear and logical, and one which has been developed through appropriate consideration of standards, guidance, and relevant good practice. The approach followed within the PCSR for the structure and presentation of the internal hazards safety case may be the basis of the shortfalls identified as in a number of cases there is detailed supporting information presented within the references. As a result, the GDA Issues should be relatively straightforward to address and I do not perceive them to result in significant shortfalls in the case as presented within the PCSR.

487 Throughout Step 4 Westinghouse have adopted a reactive approach to addressing the shortfalls. This led to documentation being produced in response to assessment concerns, and this documentation being supplied in parallel with the assessment. This may also explain some of the inconsistency I have identified within the PCSR documentation of the internal hazards safety case. The quality of the information provided coupled with the technical exchanges that have taken place during Step 4 has improved significantly from Step 3. Westinghouse has a far clearer understanding of the UK regulatory regime as well as of the approach taken to safety case production for internal hazards. It should be recognised that the approach taken within the US does not include consideration of internal hazards as a discrete part of the safety case. The approach taken is to assess the hazards as part of the work done within individual engineering disciplines, therefore, drawing all the information together in a coherent manner has proved to be a significant undertaking.

488 In all areas of my assessment where GDA Issues have been identified, Westinghouse has understood my concerns and believes that they are largely attributable to the differing regulatory approaches between the US and the UK. I expect Westinghouse to provide more detailed analysis in support of the PCSR for GDA and Westinghouse has accepted that GDA Issues are the most appropriate mechanism to address the safety case shortfalls identified as a result of my Internal Hazards Assessment.

489 In my opinion, based upon the information provided in the PCSR and supporting documentation submitted as part of the GDA process, there are no fundamental reasons for believing that a satisfactory safety case cannot be made for the generic AP1000 reactor design, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward work programme for this reactor. It must also be recognised that some of these GDA issues may ultimately require changes to the plant design. It is therefore too early to rule out the need for changes to plant layout or the provision of additional safety systems.

5.1 Key Findings from the Step 4 Assessment

490 The approach taken to the production of the safety case for internal fire is in line with my expectations and is consistent with the both national and international standards and guidance. The Fire Hazard Analysis provides detailed assessment of the potential consequences of fire including detailed analysis of plant and equipment that is assumed to fail in fire. The AP1000 design also includes detailed consideration of common cause failure and spurious operation of plant and equipment in the event of fire. The only concern identified within my assessment has been associated with the substantiation of the barriers and the associated fire dampers.

491 The PCSR and supporting references do not make it clear what provisions are in place to protect against the effects of pressure part failure which may be in part due to the incomplete pipe rupture analysis needed to inform the safety case in this area. Westinghouse has identified this concern and believes that this is based upon a different approach between the US and the UK. Notwithstanding this, the assessment of the information provided associated with the pipe rupture analysis currently being undertaken, provides a great deal of confidence that the potential pressure part failures will be captured and marshalled accordingly.

492 My assessment of internal explosion focused on two areas where there was the potential for an internal explosion; the hydrogen distribution system and the battery rooms. Although the analysis presented within the PCSR identified potential sources of explosions, I am not satisfied that the PCSR adequately presented a multi-legged argument associated with the systems in place to prevent, protect and mitigate the potential consequences. During Step 4, Westinghouse recognised the shortfall in the safety case and accepts that there is a need to provide a structured safety case in the area of internal explosion.

493 My assessment of internal missile has identified a number of shortfalls associated with the identification of potential missiles, the methods of prevention and protection and the approach to adequately capturing the claims, arguments and evidence within the safety case. Westinghouse has identified this concern and believes that this is based upon a different approach between the US and the UK and the need to provide further more detailed analysis in support of the PCSR for GDA.

494 My assessment has identified that the statements contained within the current PCSR relating to dropped loads and impact relating to the need to substantiate civil structures is to be removed from the next revision of the PCSR and be replaced with a claim relating to the preclusion of dropped loads and impact through the use of a single failure proof crane. I do not accept that such high reliability claims are appropriate with adequate substantiation of the assessment of the consequences of failure. There is a compelling case, as confirmed within current guidance and standards, operating experience and relevant good practice, in support of the need to undertake a detailed quantitative analysis of the potential consequences of a dropped load or impact arising from the use of lifting equipment. My conclusions were also subject to discussion with ND specialists within the mechanical engineering discipline who concur with my opinion within this area.

5.1.1 Assessment Findings

495 I conclude that the 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

496 I conclude that the GDA Issues listed in Annex 2 must be satisfactorily addressed before Consent will be granted for the commencement of nuclear island safety related construction.

6 REFERENCES

1 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-793 Revision A. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/23783.

2 The Master Submission List. UKP-GW-GLX-001 Revision 0. Westinghouse Electric Company LLC. April 2011. TRIM Ref. 2011/246930.

3 *ND BMS. Assessment Process.* AST/001 Issue 4. HSE. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/**ast001**.htm.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition. Revision 1. HSE. January 2008. TRIM Ref. 2007/44121.

5 *GDA Step 4 Internal Hazards Assessment Plan for the Westinghouse AP1000.* HSE-ND Assessment Plan AR 09/068. December 2009. TRIM Ref. 2009/449193.

6 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732 Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/23759.

7 *Nuclear power station generic design assessment – guidance to requesting parties.* Version 3. HSE. August 2008. http://www.hse.gov.uk/newreactors/guidance.htm.

8 *ND BMS. Technical Assessment Guide. Internal Hazards.* T/AST/014 Issue 2. HSE. August 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast014.htm .

9 *ND BMS. Technical Assessment Guide. Diversity, Redundancy, Segregation and Layout of Mechanical Plant.* T/AST/036, Issue 2. HSE. June 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast036.htm.

10 *ND BMS. Technical Assessment Guide. Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.* T/AST/051 Issue 1. HSE. May 2002. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast051.pdf.

11 *Safety of Nuclear Power Plants: Design. Safety Requirements.* Safety Standards Series No. NS-R-1. International Atomic Energy Agency (IAEA). 2000.

12 *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide.* Safety Standards Series No. NS-G-1.7 International Atomic Energy Agency (IAEA). 2004.

13 *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide.* Safety Standards Series No. NS-G-1.11. International Atomic Energy Agency (IAEA). 2004.

14 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. Issue S: Protection Against Internal Fires.* WENRA. January 2008.

15 *AP1000 Internal Hazards Topic Report*. UKP-GW-GLR-001 Revision 1. Westinghouse Electric Company LLC. February 2010. TRIM Ref. 2011/79948.

16 *AP1000 Internal Hazards Topic Report*. UKP-GW-GLR-001 Revision 2. Westinghouse Electric Company LLC. September 2010. TRIM Ref. 2011/82083.

17 *Step 3 Internal Hazards Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/016. November 2009. TRIM Ref. 2009/337472.

18 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732 Revision 1. Letter to ND from AP1000 Project Front Office. 6 April 2009. TRIM Ref. 2009/151068.

19 *AP1000 European Design Control Document*, EPS-GW-GL-700 Revision 0. February 2009, Westinghouse Electric Company LLC. TRIM Ref. 2011/384090.

20 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600724.

21 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600721.

22 AP1000 Barrier Matrix, APP-1000-GEC-004, Revision A, Westinghouse Electric Company LLC. February 2010. TRIM Ref. 2011/79762.

23 Westinghouse AP1000 – Assessment of Internal Hazards (Internal Fire, Explosions and Missiles) Issue 1. 5094126/11/001. ATKINS. 18 June 2010. TRIM Ref. 2010/278990.

24 AP1000 Barrier Matrix, APP-1000-GEC-004, Revision B, Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/73696.

25 *AP1000 UK Safety Categorisation and Classification of Structures, Systems and /Components*. UKP-GW-GL-144. Revision 0. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/173965.

26 *AP1000 European Design Control Document*, EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC.

27 Westinghouse AP1000 Nuclear Reactor, Independent Review of Internal Hazards Topic Report, Frazer-Nash Consultancy Issue 1. FNC37709/36629R. 5 May 2010. TRIM Ref. 2010/203221.

28 *Doors Functional Requirements*. APP-AD-A1-001 Revision A. Westinghouse Electric Company LLC. April 2009. TRIM Ref. 2011/90568.

29 *BS EN 13501-1:2002. Fire classification of construction products and building elements: Classification using data from reaction to fire tests.* British Standards Institution (BSi). March 2002.

30 *Standard review plan for the review of safety analysis reports for nuclear power plants.* NUREG 0800. United States Nuclear Regulatory Commission (US NRC).

31 *The Building Regulations 2006: Approved Document B: Fire*. December 2006. ISBN 978 1 85946 261 4.

32 *BS 9999:2008. Code of practice for fire safety in the design, management and use of buildings.* British Standards Institution (BSi). October 2008.

33 *BS EN 1363-1:1999. Fire resistance tests: General requirements.* British Standards Institute (BSi). November 1999.

34 *BS 476-31.1:1983. Fire tests on building materials and structures. Methods for measuring smoke penetration through doorsets and shutter assemblies. Method of measurement under ambient temperature condition*. British Standards Institute (BSi). October 1983.

35 *LPS 1056 Issue 3. Requirements and Tests for Fire Doors of at Least Two Hours Fire Resistance*. LPCB Loss Prevention Standards (LPS).

36 *ISO 10294-1. Fire Resistance Tests – Fire Dampers for Air Distribution Systems*. International Organization for Standardization. 1996.

37 *BS EN 1366-2:1999. Fire resistance tests for service installations. Part 2: Fire dampers.* British Standards Institute (BSi). November 1999.

38 *BS EN 1366-3:2009. Fire resistance tests for service installations. Part 3: Penetration seals.* British Standards Institute (BSi). March 2009.

39 *BS 476-22:1987. Fire test on building materials and structures. Methods for determination of the fire resistance of non-loadbearing elements of construction.* British Standards Institute (BSi). May 1987.

40 *BS EN 1634-1. 2008. Fire resistance test for doors and shutter assemblies- Part 1: Fire doors and shutter. British Standards Institute (BSi). May 2009.*

41 *Raceway Filling Report Auxiliary Building Elevation 66' 6.* APP-1210-ERR-001 Revision 4. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/117527.

42 *AP1000 Fire Induced Multiple Spurious Actuation Report.* APP-FPS-G1R-002 Revision 1. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/173940.

43 *Fire Protection Rule (45 FR 76602, 11/19/80). US NRC Generic Letter 81-12. United States Nuclear Regulatory Commission (US NRC). February 1981.*

44 *Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-006 Revision 0. TRIM Ref. 2010/581525.

45 *Step 4 Reactor Chemistry Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-008 Revision 0. TRIM Ref. 2010/581523.

46 *IEEE Std 484*. *Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications*. Institute of Electrical and Electronics Engineers (IEEE). February 2003.

47 *BS 6133:1995 (Ref. 47). Code of practice for safe operation of lead-acid stationary batteries.* British Standards Institute (BSi). June 1995.

48 *Step 4 Mechanical Engineering Assessment of the Westinghouse AP1000® Reactor.* ONR Assessment Report ONR-GDA-AR-11-010 Revision 0. TRIM Ref. 2010/581521.

49 *NRC Collection of Abbreviations.* NUREG-0554 Revision 4. United States Nuclear Regulatory Commission (US NRC). July 1998.

50 *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* ANSI/ASME NOG-1:1998. American Society of Mechanical Engineers (ASME). January 1998. ISBN: 0791825841.

51 *Control of Heavy Loads at Nuclear Power Plants: Resolution of Generic Technical Activity A-36.* NUREG-0612. United States Nuclear Regulatory Commission (US NRC). July 1980.

52 *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774. United States Nuclear Regulatory Commission (US NRC). July 2003.

53 *Step 4 Electrical Engineering Assessment of the Westinghouse AP1000® Reactor.* ONR Assessment Report ONR-GDA-AR-11-007 Revision 0. TRIM Ref. 2010/581524.

54 *Applicability of the Control of Major Accident Hazards Regulations (COMAH) to AP1000.* UKP-GW-GL-037 Revision 0. Westinghouse Electric Company LLC. January 2010. TRIM Ref. 2011/173945.

55 *AP1000 UK Safety Categorisation and Classification Methodology*. UKP-GW-GL-044 Revision 1. Westinghouse Electric Company LLC. April 2010. TRIM Ref. 2011/173949.

56 *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. 2011/82081.

57 *General Fire precautions, CDM in Design, Security and Internal Hazards Workshop.* Letter to Mr Robert P Jordan P.E Westinghouse Programme Manager. Letter from ND to AP1000 Joint Programme Office. WEC70277N. 14 December 2010. TRIM Ref. 2010/628960.

58 *Regulatory Reform (Fire Safety) Order 2005*. Statutory Instrument No. 1541. Regulatory Reform, England and Wales. June 2005.

59 *Construction (Design and Management) Regulations 2007*. Statutory Instrument No. 320. Health and Safety Executive. February 2007.

Table 1

Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4

SAP No.	SAP Title	Description
SC.4	Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
EKP.3	Defence in depth	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 levels of protection.
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	Safety Measure	Safety measures should be identified to deliver the required safety function(s).
ECS.1	Safety Categorisation	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.
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.
EDR.2	Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.
EDR.4	Single failure criterion	During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.
ELO.4	Minimisation of the effects of incidents	The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.

Table 1

Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4

SAP No.	SAP Title	Description
EHA.1	Identification	External and Internal Hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.
EHA.3	Design basis events	For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.
EHA.4	Frequency of exceedance	The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance in accordance with the fault analysis requirements (FA.5).
EHA.5	Operating conditions	Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.
EHA.6	Analysis	Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.
EHA.7	'Cliff-edge' effects	A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences.
EHA.10	Electromagnetic interference	The design of facility should include protective measures against the effects of electromagnetic interference.
EHA.13	Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials	The on-site use, storage or generation of hazardous materials should be minimised, and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility.
EHA.14	Fire, explosion, missiles, toxic gases etc – sources of harm	Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.

Table 1

Relevant Safety Assessment Principles for Internal Hazards Considered During Step 4

SAP No.	SAP Title	Description
EHA.15	Fire, explosion, missiles, toxic gases etc – effects of water	The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.
EHA.16	Fire, explosion, missiles, toxic gases etc – fire detection and fighting	Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.
FA.6	Fault sequences	For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Internal Hazards – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-IH-01	The licensee shall, during the specification of the barrier penetrations as part of the detailed design studies, provide evidence to support that the method of barrier sealing is able to meet the 3 hour fire resistance requirements for insulation and integrity in accordance with the requirements stated within the PCSR.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-AP1000-IH-02	The Licensee shall provide evidence of the management procedures to demonstrate that the cable tray loadings are managed to ensure that the fill limits as detailed within the PCSR as maintained below the requisite levels stated within the design.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-AP1000-IH-03	The Licensee shall provide analyses in line with that undertaken within Westinghouse report, *"Raceway Filling Report Auxiliary Building Elevation 66' 6"*, APP-1210-ERR-001 (Ref. 41) as part of the site specific PCSR for all cable trays that contain cabling which performs a Class 1 safety function, with the exception of those cable trays contained within fire rated enclosures or that are provided with passive fire protection.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-AP1000-IH-04	The Licensee shall provide details of all cable routes provided with passive fire protection as part of the site specific PCSR and furthermore, explain the basis for the application of passive fire protection and the impact on nuclear safety of the aforementioned protection.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.
AF-AP1000-IH-05	The Licensee shall identify and address any gaps and inconsistency between the Internal Hazards aspects of the PCSR and the AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – inactive commissioning.

Annex 1

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 – Internal Hazards – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
INTERNAL FIRE SAFETY CASE SUBSTANTIATION
GI-AP1000-IH-01 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Civil Engineering		
GDA Issue Reference	**GI-AP1000-IH-01**	**GDA Issue Action Reference**	**GI-AP1000-IH-01.A1**
GDA Issue	Internal Fire Safety Case Substantiation		
GDA Issue Action	Provide substantiation of the nuclear significant hazard barriers claimed to provide the level of fire resistance stated within the PCSR for integrity, insulation and load bearing capacity (where applicable). This may include a multi-legged argument consisting of the following: • Reference to physical fire testing or detailed supporting analysis (backed by appropriately verified and validated fire models) of the barriers and cable tray enclosures claimed. • The approach taken to minimise penetrations within the barriers. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

INTERNAL FIRE SAFETY CASE SUBSTANTIATION

GI-AP1000-IH-01 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Civil Engineering		
GDA Issue Reference	**GI-AP1000-IH-01**	**GDA Issue Action Reference**	**GI-AP1000-IH-01.A2**
GDA Issue Action	Provide the substantiation of the approach taken to the design and installation of fire dampers claimed within the AP1000 PCSR. This may include a multi-legged argument consisting of the following factors: • Details of the design approach to the installation of fire dampers within the AP1000 design. • The consideration of the single failure criterion. • Reference to the appropriate codes and standards which demonstrate the fire dampers installed will meet the requirements for 3 hours fire resistance both in terms of integrity and insulation. • Provisions associated with the application of any passive fire protection to ensure that the dampers meet insulation requirements as detailed within point 3 above.The approach taken to the control of the fire dampers both in terms of detection driven oper ensuring that full divisional segregation is met. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

INTERNAL FLOODING SAFETY CASE

GI-AP1000-IH-02 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-02**	**GDA Issue Action Reference**	**GI-AP1000-IH-02.A1**
GDA Issue	There is a need to provide an updated internal flooding safety case as there are inconsistencies associated with claims made on barriers, drains and sumps, and flood calculations.		
GDA Issue Action	Provide an updated internal flooding safety case that considers the claims, arguments and evidence associated with internal flooding. As part of the production of the aforementioned case there is a need to consider the following aspects within the safety case: • All potential unmitigated flood sources taking into account bounding flood sources and volumes. • The barriers claimed to provide segregation of safety significant SSCs in the event of internal flooding. • Any claims made on drainage systems, sumps, drains, flow paths etc and arguments and evidence provided to demonstrate that they will be available for postulated internal flooding events. • Any claims made on pressure relief panels and compartment vents need to supported by arguments and evidence to demonstrate that they will be available for postulated internal flooding events. • Any ALARP claims made on operator actions in relation to the mitigation of potential flood events rather than assuming operator success as part of the deterministic case. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PRESSURE PART FAILURE

GI-AP1000-IH-03 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Structural Integrity		
GDA Issue Reference	**GI-AP1000-IH-03**	**GDA Issue Action Reference**	**GI-AP1000-IH-03.A1**
GDA Issue	Provide substantiation to support claims and arguments made within the area of pressure part failure.		
GDA Issue Action	Identify and substantiate all nuclear significant pipe whip restraints, barriers and shields claimed for the protection of redundant trains against the effects of pressure part failure. This substantiation should take consideration of the following: • Quantitative assessment of the consequences of postulated pipe failures (including high energy pipework that is not claimed as HSS derived from the pipe rupture analysis. • Justification of the method applied to selection of the type of protection adopted e.g. pipe restraint, barrier or shield. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PRESSURE PART FAILURE

GI-AP1000-IH-03 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Structural Integrity		
GDA Issue Reference	**GI-AP1000-IH-03**	**GDA Issue Action Reference**	**GI-AP1000-IH-03.A2**
GDA Issue Action	Provide the updated safety case that details the identification and substantiation of all claims made in relation to Main Steam Isolation Compartments associated with pressure part failure. This substantiation should take consideration of the following: • Structural integrity claims made on the main steam line and feedwater line pipework. • Engineered design provisions in place to either prevent or mitigate the potential consequences of pipe failure within the two MSIV Compartments e.g. pressure relief paths, valve actuation etc. • Whether there is a requirement for passive features such as pipewhip restraints, barriers or shields. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
INTERNAL EXPLOSION SAFETY CASE SUBSTANTIATION
GI-AP1000-IH-04 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-04**	**GDA Issue Action Reference**	**GI-AP1000-IH-04.A1**
GDA Issue	Provide substantiation to support claims and arguments made within the area of internal explosion.		
GDA Issue Action	Provide substantiation of the safety case for explosion within Battery Rooms. This should include consideration of a multi-legged argument associated with the following: • Potential hydrogen accumulation rates during normal and fault conditions. • Consideration of heating, ventilation, and air conditioning (HVAC) systems. • Hydrogen detection. • Engineered protection systems associated with the cessation of battery charging. • Civil structures in place to prevent propagation of a hydrogen explosion to redundant trains of protection. Administrative controls or procedures presented as risk mitigation. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
INTERNAL EXPLOSION SAFETY CASE SUBSTANTIATION
GI-AP1000-IH-04 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-04**	**GDA Issue Action Reference**	**GI-AP1000-IH-04.A2**
GDA Issue Action	Provide substantiation of the safety case for the routing of the hydrogen pipework within areas containing Class 1 SSCs. This should include consideration of a multi-legged argument associated with the following: • Potential hydrogen accumulation rates during normal and fault conditions. • Consideration of heating, ventilation, and air conditioning (HVAC) systems. • Hydrogen detection. • Civil structures in place to prevent propagation of a hydrogen explosion to redundant trains of protection. • Administrative controls or procedures presented as risk mitigation. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

INTERNAL MISSILE SAFETY CASE

GI-AP1000-IH-05 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-IH-05**	**GDA Issue Action Reference**	**GI-AP1000-IH-05.A1**
GDA Issue	Identify and substantiate the claims, arguments and evidence that constitute the internal missile aspects of the internal hazards safety case.		
GDA Issue Action	Identify and substantiate the claims, arguments and evidence that constitute the internal missile aspects of the internal hazards safety case. This substantiation should take consideration of the following: • Identification of all potential areas where missiles could result in loss of more than one division or train of protection, including failures associated with pressure part failure. • Analysis of the potential consequences associated with internal missile generation. • The identification and substantiation of all engineered prevention features e.g. component integrity, overspeed systems, trip functions etc. claimed for the protection of redundant trains against the effects of internally generated missiles. • The identification and substantiation of all nuclear significant hazard barriers claimed for the protection of redundant trains against the effects of internally generated missiles. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SUBSTANTIATION AND ANALYSIS OF THE CONSEQUENCES OF DROPPED LOADS AND IMPACT FROM LIFTING EQUIPMENT INCLUDED WITHIN THE AP1000 DESIGN

GI-AP1000-IH-06 REVISION 0

Technical Area	**INTERNAL HAZARDS**		
Related Technical Areas	Mechanical Engineering		
GDA Issue Reference	**GI-AP1000-IH-06**	**GDA Issue Action Reference**	**GI-AP1000-IH-06.A1**
GDA Issue	Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment included within the AP1000 design.		
GDA Issue Action	Identify and substantiate all claims made on SSCs associated against the effects of dropped load and impact. This approach should, in the first instance, consider the potential consequences of a dropped load or impact on a quantitative basis to determine significance of the dropped load or impact. This should then lead to detailed multi-legged arguments to demonstrate that the provisions in place to ensure that the risk to nuclear safety of a load drop or impact was ALARP and that such analysis may take into account: • Claims on civil structures. • Additional physical protection. • Limits and conditions on the use of the lifting equipment. • Provision of detailed load path routes avoiding areas of highest nuclear significance. • Measures (both system based and administratively controlled) in place to ensure the potential for impact of the load is minimised. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform Westinghouse of my expectations. With agreement from the Regulator this action may be completed by alternative means.		