Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 INTERNAL HAZARDS ASSESSMENT OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/016-P

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

EXECUTIVE SUMMARY

This report presents the findings of the internal hazards assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Generic Design Assessment (GDA) process.

This report for the Westinghouse AP1000 presents the results of Nuclear Directorate's (ND) Step 3 assessment of internal hazards. It provides an overview of the safety case presented in the PCSR; the standards and criteria adopted in the assessment; and an assessment of the claims and arguments provided within the safety case.

The scope of the internal hazards assessment is detailed within the Project Initiation Document (PID), GDA Phase 1 – Steps 3 and 4 Internal Hazards Assessment Strategy (Ref. 2). The PID states that Step 3 is a review of the safety aspects of the proposed reactor designs by undertaking an assessment primarily at the system level and assessment of the supporting arguments made in the Requesting Party's (RPs) Pre Construction Safety Report (PCSR).

The approach to the structure of this assessment report for Step 3 was to first confirm, or otherwise, that the observations made during the Step 2 phase of the GDA process had been addressed or adequately captured through further technical queries, regulatory observations or through the continuation of the assessment into Step 4. Secondly, there was a need to undertake internal hazards assessment on the claims and arguments contained within the PCSR and other supporting documents that had been produced by Westinghouse as part of the safety demonstration for Step 3 of the GDA process.

The PCSR and Design Control Document (DCD) (Ref. 9) for the AP1000 have been presented in a structure that is not in line with the expectations of the UK Regulator. This was identified during Step 3 and Westinghouse (WEC) committed to produce an Internal Hazards Topic Report (Ref. 11) whose scope was to present the safety case for internal hazards in a claims, arguments and evidence structure. The Internal Hazards Topic Report has now been issued to ND, however, there has been insufficient time prior to the end of Step 3 for a detailed assessment to be undertaken. A number of comments made within this Step 3 Internal Hazards Assessment Report relating to the requirement for a detailed structured case will need to be either addressed by WEC in the Internal Hazards Topic Report or be scheduled to be addressed elsewhere during Step 4. It is the intention to undertake a detailed assessment of the Internal Hazards Topic Report within Step 4 of the GDA process.

It is important to stress that not all areas have been assessed to the same extent due to the sampling nature of the assessment and due to the limited detailed information contained within the PCSR and DCD.

I conclude that the safety case provided by the Westinghouse has significant shortfalls. My assessment has identified areas where further work will be required before the safety case can be considered acceptable. I consider that there is a need for Westinghouse to address the concerns relating to the lack of detailed claims and arguments presented during Step 3 coupled with the need to provide sufficient evidence during Step 4 in order to produce an adequate safety case submission for internal hazards. The Internal Hazards Topic Report appears to be the mechanism by which this will be demonstrated, however, this has yet to be assessed in detail by ND.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
BMS	(Nuclear Directorate) Business Management System
CCS	Component Cooling Water System
DBA	Design Basis Accident
DCD	Design Control Document
EA	The Environment Agency
ESFs	Engineered Safety Features
FPS	Fire Protection System
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
LOCA	Loss of Coolant Accident
MCR	Main Control Room
ND	The (HSE) Nuclear Directorate
PCER	Pre-construction Environment Report
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PCCWST	Passive Containment Cooling Water Storage Tank
PID	Project Initiation Document
RCP	Reactor Coolant Pump
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
SAP	Safety Assessment Principle
SSC	Structure, System and Component
SSE	Safe Shutdown Earthquake
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
WEC	Westinghouse Electric Company LLC
WENRA	The Western European Nuclear Regulators' Association

TABLE OF CONTENTS

1 INTRODUCTION

1 This report presents the findings of the internal hazards assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) undertaken as part of Step 3 of the Generic Design Assessment (GDA) process. This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 3) and its associated guidance document G/AST/001 (Ref. 4). AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 5) have been used as the basis for the assessment of the internal hazards associated with AP1000 design. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 This internal hazards assessment report for the AP1000 provides an overview of the safety case in the form of the PCSR as produced by Westinghouse, the standards and criteria adopted in the assessment undertaken by ND and an assessment of the claims and arguments provided within the safety case based upon those standards and criteria. This structure of this assessment report is in accordance with the requirements of the BMS standard on assessment reports (Ref. 6) taking due cognisance of the guidance within the BMS relating to assessment report production (Ref. 7).

3 The approach to the structure of this assessment report for Step 3 was to first confirm, or otherwise, that the observations made during the Step 2 phase of the GDA process had been addressed or adequately captured through further technical queries, regulatory observations or through the continuation of the assessment into Step 4. Secondly, there was a need to undertake internal hazards assessment on the claims and arguments contained within the PCSR and other supporting documents that had been produced by Westinghouse as part of the safety demonstration for Step 3 of the GDA process.

4 It is important to stress that not all areas have been assessed to the same extent due to the sampling nature of the assessment and due to the limited detailed information contained within the PCSR and DCD.

5 The scope of the internal hazards assessment is detailed within the Project Initiation Document (PID), GDA Phase 1 – Steps 3 and 4 Internal Hazards Assessment Strategy (Ref. 2). The PID states that Step 3 is a review of the safety aspects of the proposed reactor designs by undertaking an assessment primarily at the system level and assessment of the supporting arguments made in the requesting parties' (RPs) Pre-Construction Safety Report (PCSR).

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

6 The internal hazards aspects of the PCSR for the Westinghouse AP1000 address the method by which internal hazards are identified, the process applied in the assessment of internal hazards, and an overview of the principle claims made to protect the plant against the effects of the identified internal hazards. Each hazard is addressed specifically within the PCSR with reference back to the Design Control Document (DCD) (Ref. 9) to provide further detailed information. The hazards specifically addressed within the PCSR are:

- Internal Flooding.
- Missile Protection.
- Pipewhip.
- Spray.
- Fire.
- Toxic / Asphyxiant Gases.
- Explosion.
- Release of Corrosive Substances.
- Collapsing/Falling Loads.

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

2.1.1 Internal Flooding

8 The PCSR states the high level claims for internal flooding associated with systems classified as Safety-Related and involves the provision of sufficient redundancy and segregation such that loss of one train will not affect overall functionality, or that these systems have been located above the highest potential flood level.

9 Further supporting information is provided within Chapter 3.4 of the DCD which is further explained below.

10 The AP1000 arrangement provides physical separation of redundant safety-related components and systems from each other and from non safety-related components. As a result, component failures resulting from internal flooding do not prevent safe shutdown of the plant or prevent mitigation of the flooding event. The protection mechanisms related to minimising the consequences of internal flooding include the following:

- Structural enclosures.
- Structural barriers.
- Curbs and elevated thresholds.
- Leak detection systems.
- Drain systems.

11 The AP1000 minimises the number of penetrations through enclosure or barrier walls below the flood level. Those few penetrations through flood protection walls that are below the maximum flood level are watertight. Any process piping penetrating below the maximum flood level either is embedded in the wall or floor or is welded to a steel sleeve embedded in the wall or floor. There are no watertight doors in the AP1000 used for

internal flood protection because they are not needed to protect safe shutdown components from the effects of internal flooding. The walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads associated with a pipe failure. The two watertight doors on the waste hold-up tank compartments limit the consequence of a failure on spent fuel pool water level.

2.1.2 Missile Protection

12 There are two fundamental criteria applied in the AP1000 for protection against internally generated missiles:

- Missiles are not to be capable of damaging Structures, Systems and Components (SSCs) to prevent safe shutdown or to result in a significant release of activity;
- Single active component failure is assumed in systems used to mitigate the effects of missiles and achieve safe shutdown, in addition to the direct consequences of the missiles; this includes offsite power being unavailable (although not losses of structural integrity).

13 Further supporting information is provided within Chapter 3.5 of the DCD which is further explained below.

14 The AP1000 criteria for protection from postulated missiles provide the capability to safely shut down the reactor and maintain it in a safe shutdown condition.

15 Missiles may be generated by pressurised components, rotating machinery, and explosions within the plant and by tornadoes or transportation accidents external to the plant. Potential missile hazards are eliminated to the extent practical by minimising the potential sources of missiles through proper selection of equipment, and by arrangement of structures and equipment in a manner to minimise the potential for damage from missiles.

16 The following criteria are applied in the identification of missiles and the protection requirements that must be satisfied:

- A missile must not damage structures, systems, or components to the extent that could prevent achieving or maintaining safe shutdown of the plant or result in a significant release of radioactivity.
- A single active component failure is assumed in systems used to mitigate the consequences of the postulated missile and achieve a safe shutdown condition. The single active component failure is assumed to occur in addition to the postulated missile and any direct consequences of the missile.
- Walls, partitions, and other items that enclose safety-related systems, or separate redundant trains of Safety-Related equipment, must be constructed so that a postulated missile cannot damage components required to achieve safe shutdown nor damage components required to prevent a release of radioactivity.
- A postulated missile from the reactor coolant system must not cause loss of integrity of the primary containment, main steam, feedwater, or other loop of the reactor coolant system.
- A postulated missile from any system other than the reactor coolant system must not cause loss of integrity of the containment or the reactor coolant system pressure boundary.
- Other plant accidents or severe natural phenomena are not assumed to occur in conjunction with a postulated missile.

- Offsite power is assumed to be unavailable if a trip of the turbine-generator or reactor protection system is a direct consequence of the postulated missile.
- Safe shutdown is accomplished using only safety-related systems with a coincident single active failure, although non safety-related systems not affected by the missile are available to support safe shutdown.
- Missiles are postulated to occur where the single failure of a retention mechanism can result in a missile, unless the missile is not considered credible. Missiles created by the independent failures of two retention mechanisms are not postulated.
- The energy of postulated missiles produced by rotating components is based on a 120 percent overspeed condition, unless such an overspeed condition is not possible (such as a synchronous motor).
- Equipment required for safe shutdown is located in plant areas separate from potential missile sources wherever practical.
- Spatial separation may be used to demonstrate protection from missile hazards when it is shown that the range and trajectory of the generated missile is less than the distance to or is directed away from the potential target.

17 The AP1000 passive design minimises the number of safety-related structures, systems, and components required for safe shutdown. The areas required for safe shutdown, and the major systems and components housed therein that are required to be protected from internally and externally generated missiles for safe shutdown, are summarized below:

- The containment vessel, including the reactor coolant loop, and passive core cooling system inside containment.
- The shield building, including the passive containment cooling system.
- Containment penetration areas, including containment isolation valves and Class IE cables.
- The control complex including the main control room, reactor protection system, batteries, and dc switchgear.
- The spent fuel pit.

18 The AP1000 relies on safety-related systems and equipment to establish and maintain safe shutdown conditions. There are no non safety-related systems or components that require protection from missiles.

19 Evaluations are performed to demonstrate that the criteria are satisfied in the event a credible missile is produced coincident with a single active component failure. These evaluations include the following:

- For those potential missiles considered to be credible, a realistic assessment is made of the postulated missile size and energy, and its potential trajectories.
- Potentially impacted components associated with systems required to achieve and maintain safe shutdown are identified.
- Loss of these potentially impacted components coincident with an assumed single active component failure is evaluated to determine if sufficient redundancy remains to achieve and maintain a safe shutdown condition. If these criteria are satisfied, no further protection is required for the identified missile. If these conditions are not satisfied, additional protective features are incorporated (for example, plant layout is modified, or barriers are added).

2.1.2.1 Evaluation of Internally Generated Missiles (Outside Containment)

20 The consideration of missile sources outside containment that can adversely affect safety-related structures, systems or components is limited to a few rotating components inside the auxiliary building and a few pressurised components in the chemical volume and control system. The safety-related systems and components needed to bring the plant to a safe shutdown are located inside the containment shield building and auxiliary building, both of which have thick structural concrete exterior walls that provide protection from missiles generated in other portions of the plant. Safety-related systems and components located in the auxiliary building, including the main control room, are protected from missiles generated in other portions of the auxiliary building by the structural concrete interior walls and floors.

21 Rotating components located inside the auxiliary building that are either safety-related or are constructed as canned motor pumps would contain fragments from a postulated fracture of the rotating elements. These are excluded from evaluation as missile sources. Rotating components used less than 2 percent of the time are also excluded from evaluation as missile sources. This exclusion of equipment that is used for a limited time is similar to the approach used for the definition of high-energy systems. Non safety-related rotating equipment in compartments surrounded by structural concrete walls with no safety-related systems or components inside the compartment is not considered a missile source. Rotating equipment within a housing or an enclosure that contains the fragments of a postulated impeller failure is not considered a credible source of missiles. For one or more of these reasons the non safety-related rotating equipment inside the auxiliary building is not considered to be a credible missile source. Non safety-related rotating equipment in compartments with safety-related systems or components that do not provide other separation features have design requirements for a housing or an enclosure to retain fragments from postulated failures of rotating elements.

22 Falling objects (i.e. gravitational missiles) 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 safety-related structures, systems, and components. Safety-related structures, systems, or components are protected from non-seismically designed structures, systems, or components or the interaction is evaluated. Valves, rotating equipment, vessels, and small fittings not otherwise considered to be credible missiles due to design features or other considerations are not considered to be a potential source of missiles when struck by a falling object. The air storage bottles are located within a structural steel frame and are in an area with no activity directly above. For the reasons noted above, secondary missiles are not considered credible missiles.

2.1.2.2 Evaluation of Internally Generated Missiles (Inside Containment)

23 The consideration of credible missile sources inside containment that can adversely affect Safety-Related structures, systems, or components is limited to a few rotating components. The Safety-Related systems and components needed to bring the plant to a safe shutdown are inside the containment shield building and auxiliary building both of which have thick structural concrete exterior walls that provide protection from missiles generated in other portions of the plant.

24 Rotating components inside containment that are either safety-related or are constructed as seal-less pumps would contain fragments from a postulated fracture of the rotating elements and are excluded from evaluation as missile sources. Rotating components in use less than 2 percent of the time are also excluded from evaluation as missile sources. This exclusion of equipment that is used for a limited time is similar to the approach used for the definition of high-energy systems. This includes the reactor coolant drain pumps, the containment sump pumps and motors for valve operators, and mechanical handling

equipment. Non-safety-related rotating equipment in compartments surrounded by structural concrete walls with no safety-related systems or components inside the compartment is not considered a missile source. Rotating equipment with a housing or an enclosure that contains the fragments of a postulated impeller failure is not considered a credible source of missiles. For one or more of these reasons the non-safety-related rotating equipment inside containment is considered not to be a credible missile source. Non safety-related rotating equipment in compartments with safety-related systems or components that do not provide other separation features has design requirements for a housing or an enclosure to retain fragments from postulated failures of rotating elements.

25 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. 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. Valves, rotating equipment, vessels, and small fittings not otherwise considered to be credible missiles due to design features or other considerations are not considered to be a potential source of missiles when struck by a falling object. Secondary missiles are not considered credible. Striking a component with a falling object will not generate a secondary missile if design of the component precludes generation of missiles due to pressurization of the component. Safety-related structures, systems, or components are protected from non-seismically designed structures, systems, or components or the interaction is evaluated. Non safety-related equipment that could fall and damage safety-related equipment during an earthquake is classified as seismic Category II and is designed and supported to preclude such failure. There are no high-pressure gas storage cylinders inside the containment shield building. For the reasons noted above, secondary missiles are not considered credible missiles.

2.1.3 Pipewhip

26 Systems designated essential for safe shutdown in the event of pipe rupture, where in proximity to pipework that has not been assessed to demonstrate leak before break, are protected from the effects of pipewhip by distance, protective barriers, and pipe restraints which are appropriately qualified. Those systems designated essential for safe shutdown in the event of pipe failure are:

- Reactor coolant system.
- Steam generator system.
- Passive cooling system.
- Protection and safety monitoring system.
- Class 1E dc.
- Uninterruptible power supply.
- Main Control Room and associated habitability systems.
- Containment penetrations and isolation valves.

27 Further supporting information is provided within Chapter 3.6 of the DCD which is further explained below.

28 An analysis of postulated pipe failures is performed to determine the impact of such failures on those safety-related systems or components that provide protective actions and are required to mitigate the consequences of the failure. Through such protective measures, as separation, barriers, and pipewhip restraints, the effects of breaks, through-wall cracks, and leakage cracks are prevented from damaging essential items to an

extent that would impair their essential function or necessary component operability. The capability of specific safety-related systems to withstand a single active failure concurrent with the postulated event is discussed, as applicable. When the results of the pipe failure effects analysis show that the effects of a postulated pipe failure are isolated, physically remote, or restrained by protective measures from essential systems or components, no further dynamic analysis is performed.

29 The plant arrangement is based on maximizing the physical separation of redundant or diverse safety-related components and systems from each other and from non safety-related items. Therefore, in the event a pipe failure occurs, there is a minimal effect on other essential systems or components required for safe shutdown of the plant or to mitigate the consequences of the failure. The effects associated with a particular pipe failure are mechanistically consistent with the failure. Thus, pipe dimensions, piping layouts, material properties, and equipment arrangements are considered in defining the specific measures for protection against the consequences of postulated failures. Protection against the dynamic effects of pipe failures is provided by physical separation of systems and components, barriers, equipment shields, and pipewhip restraints. The precise method chosen depends largely upon considerations such as accessibility and maintenance. The preferred method of providing protection is by separation. When separation is not practical pipewhip restraints are used. Barriers or shields are used when neither separation nor pipewhip restraints are practical. This protection is not required when piping satisfies leak-before-break criteria.

30 The plant arrangement provides separation, to the extent practicable, between redundant safety systems (including their appurtenances) to prevent loss of safety function as a result of events for which the system is required to be functional. Separation between redundant safety systems is the basic protective measure incorporated in the design to protect against the dynamic effects of postulated pipe failures. In general, separation is achieved by:

- Safety-related systems located remotely from high-energy piping, where practicable.
- Redundant safety systems located in separate compartments, where practicable.
- Specific components enclosed to retain the redundancy required for those systems that must function to mitigate specific piping failures.
- Drainage systems provided for flooding control.

31 Where physical separation is not possible, the pipe rupture hazard analysis includes an evaluation to determine the systems and components that require a structure for separation from the effects of a break in a high energy line. For these structures specifically included to separate breaks from essential systems or components, the evaluation considers that the break may be at the closest point in the line to the separating structure. High energy lines qualified as leak-before-break lines and the lines in containment penetration break exclusion areas are not included as possible break locations in this evaluation.

32 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, a separating structure such as additional barriers, deflectors, or shields is provided to meet the functional protection requirements. Inside the containment, the secondary shield wall serves as a barrier between the reactor coolant loops and the containment. In addition, the refuelling cavity walls, operating floor, and secondary shield walls minimize the possibility of an accident that may occur in any one reactor coolant loop affecting the other loop or the containment. Those portions of the steam and feedwater lines located within the containment are routed in such a manner that possible interaction between these lines and the reactor coolant piping is minimized. The direct vessel injection valves for train A and train B are separated by the secondary

shield wall. Barriers and shields that are identified as required by the pipe rupture hazard analysis are designed for loads from a break in the line at the closest location to the structure.

33 Measures for protection against pipewhip are provided where the unrestrained pipe movement of either end of the ruptured pipe could cause damage at an unacceptable level to any structure, system, or components required to meet the criteria outlined in this subsection.

34 The analysis of the consequences of pipe breaks, through-wall cracks, and leakage cracks uses the following criteria:

- High-energy containment penetrations are subject to special protection mechanisms. Restraints are provided to maintain the operability of the isolation valves and the integrity of the penetration due to a break in the safety-related and non safety piping beyond the restraint if required. These restraints are located as close as practicable to the containment isolation valves associated with these penetrations.
- Instrumentation required to function following a pipe rupture is protected.
- High-energy fluid system pipe whip restraints and protective measures are designed so that a postulated break in one pipe cannot lead to a rupture of other nearby essential pipes or components, if the secondary rupture results in consequences that are unacceptable for the initial postulated break.

35 For those cases in which the rupture of the main steam or feedwater piping inside containment is the postulated initiating event, the turbine control, turbine stop, moisture separator reheater 2nd stage steam isolation, and turbine bypass valves, and to a limited extent, the control systems for the turbine stop and feedwater control valves (which are non safety-related equipment), are credited in single failure analysis to mitigate the event. This equipment is not protected from pipe ruptures in the turbine building because the postulated pipe rupture for which it provides protection is inside containment. The assumed single active failure for this analysis is the function of the safety-related valve that would normally isolate the piping.

2.1.4 Spray

36 Systems designated essential for safe shutdown that are in close proximity to pipework that is not claimed as part of the leak before break argument are environmentally qualified to be protected against the effects of spray.

37 Further supporting information is provided within Chapter 3.6.2.7 of the DCD which is further explained below.

38 Essential systems and components are evaluated for the potential effects of spray from high- and moderate-energy through-wall cracks. Spray effects are assumed to be limited to the compartment where the pipe failure occurs. The spray is assumed to wet unprotected components in the compartment. It is further assumed the spray does not damage non-electrical passive components, including piping, ducts, valve bodies, or mechanical components of valve operators. Spray may cause failure of electrical components not designed to withstand wetting.

39 The safe shutdown components inside containment are subject to wetting from design basis events inside containment. These conditions bound the effects of spray from moderate energy cracks.

40 The doors to the auxiliary Class 1E battery rooms are normally closed, so spray cannot affect the batteries if fire fighting activities or a pipe crack were to occur in the corridor. If fire fighting activities were to occur in a particular room, all of the equipment is assumed inoperable due to the fire, therefore, no further spray effects need be considered. The

containment isolation valves subject to spray and the safe shutdown components in the main steam tunnels are provided with spray protection. The sensitive components of the main control room emergency habitability system are protected from spray effects.

2.1.5 Fire

41 The Fire Protection System (FPS) has been designed to provide expedient fire detection and suppression in line with the nuclear safety implications of fires in specific areas of plant; it has been designed to take consideration of the fire hazard analysis, to make sure that Safety-Related SSCs required for safe plant shutdown or to prevent significant releases of radioactive material can maintain functionality. This includes the provision of redundant trains of equipment and segregation, where required.

42 Fire Hazards Analysis has also been performed, which splits the plant into Fire Areas segregated structurally and fire zones segregated by barriers and distance. Within each area, a combustible inventory is undertaken, and the maximum temperature and duration of a fire are calculated. Conservative estimates are made of Safety-Related SSCs within the specific area that could be disabled by such a fire; as noted previously, redundant and segregated systems are specified where required to maintain essential functionality. Interfaces with other fire areas are considered; potential for fire/smoke propagation where fire barrier / fire damper duration could be exceeded is identified, and appropriate protective features incorporated against the failure of Safety-Related SSCs.

43 The PCSR states that the primary objectives of the AP1000 FPS are to prevent fires, to minimise the consequences should a fire occur and provide protection so that the plant can be shut down safely following a fire. The FPS has a Safety-Related function associated with preserving containment integrity via isolation of the FPS line penetrating the containment. No other aspects of the FPS are classified as Safety-Related.

2.1.5.1 System Description

44 The FPS detects fires and provides the capability to extinguish them using fixed automatic and manual suppression systems, manual hose streams and / or portable fire fighting equipment. The FPS consists of a number of fire detection and suppression subsystems including:

- Detection systems for early detection and notification of a fire that provide audible and visual alarms and system trouble annunciation in the Main Control Room (MCR) and the Security Central Alarm Station.
- A water supply system including two separate fresh water storage tanks, the two fire pumps, yard main and interior distribution piping.
- Fixed automatic fire suppression systems which include wet pipe, dry pipe, pre-action and deluge sprinkler or water spray systems.
- Manual fire suppression systems and equipment, including hydrants, standpipes (and / or the seismic standpipe system), hose stations and portable fire extinguishers.

45 The FPS detects and suppresses fires. It is designed to:

- Prevent fire initiation by controlling, separating and limiting the quantities of combustibles and sources of ignition.
- Isolate combustible materials and limit the spread of fire by subdividing plant buildings into fire areas separated by fire barriers.
- Separate redundant safe shutdown components and associated electrical divisions to preserve the capability to safely shut down the plant following a fire.

- Provide the capability to safely shut down the plant using controls external to the MCR, should a fire require evacuation of the control room or damage the control room circuitry for safe shutdown systems.
- Separate redundant trains of safety-related equipment used to mitigate the consequences of a design basis accident (but not required for safe shutdown following a fire) so that a fire within one train will not damage the redundant train.
- Prevent smoke, hot gases or fire suppressants from migrating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities.
- Provide confidence that failure or inadvertent operation of the FPS cannot prevent plant safety functions from being performed.
- Preclude the loss of structural support, due to warping or distortion of building structural members caused by the heat from a fire, to the extent that such a failure could adversely affect safe shutdown capabilities.
- Provide floor drains sized to remove expected fire fighting water flow without flooding Safety-Related equipment.
- Provide fire fighting personnel access and escape routes for each fire area.
- Provide emergency lighting and communications for safe shutdown following a fire.
- Minimise exposure to personnel and releases to the environment of radioactivity or hazardous chemicals as a result of a fire.

46 The FPS provides fire protection for the Nuclear Island, the Annex Building, the Turbine Building, the Radwaste Building and the Diesel Generator Building. It provides two Fire Water Storage Tanks, each capable of holding at least 1,100m^3 of water and two fire pumps provide at least 454 m^3/hr each at a total head of at least 90 m. The fire pumps maintain 100% of fire pump design capacity, assuming failure of the largest fire pump or loss of offsite power. The fuel tank for the diesel-driven fire pump is capable of holding at least 900 litres. The FPS supplies fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system plus 113 m^3/hr for fire hoses, for a minimum of 2 hours.

47 The FPS satisfies the requirements of the Passive containment Cooling System (PCS) as an alternate source of water to wet the containment dome or to refill the Passive Containment Cooling Water Storage Tank (PCCWST) after a Loss Of Coolant Accident (LOCA), if the FPS is available. The FPS provides an alternate supply of cooling water to the Normal Residual Heat Removal System (RNS) Heat Exchanger after a loss of normal Component Cooling water System (CCS) function. The engineering of the AP1000 against fire includes the passive protection provided by the structure and the active protection provided by the FPS.

2.1.5.2 Passive Architectural and Structural Features

48 The design of the AP1000 plant buildings uses non-combustible structural materials, primarily reinforced concrete, gypsum, masonry block, structural steel, steel siding and concrete / steel composite material. Localised structural steel fireproofing is provided as required, based on a realistic analysis of the time-temperature fire effects on the structural members determined by heat transfer analyses based on the postulated fire. Fire fighting personnel access routes and safety escape routes are provided for each fire area.

2.1.5.3 Plant Arrangement

49 The plant is subdivided into fire areas to isolate potential fires and minimise the risk of the spread of fire and the resultant consequential damage from corrosive gases, fire suppression agents, smoke and radioactive contamination. Some of the fire areas are further subdivided into fire zones.

50 Three-hour fire barriers provide complete separation of redundant safe shutdown components, including equipment, electrical cables, instrumentation and controls, except where the need for physical separation conflicts with other important requirements, specifically:

- Fire barrier separation is not provided within the MCR fire area because functional requirements make such separation impractical,
- Fire barrier separation is not provided between the MCR and the room above it from fires in the MCR as there are no safe shutdown components in the room above,
- Fire barrier separation is not provided within the remote shutdown room fire area because the remote shutdown workstation is not required for safe shutdown unless a fire requires evacuation of the MCR,
- Complete fire barrier separation necessary to define a fire area is not provided throughout the primary containment fire area (including the middle and upper annulus zones of the Shield Building) because of the need to satisfy other design requirements, such as allowing for pressure equalisation within the containment following a high-energy line break.

51 Outside of the primary containment and the MCR, the arrangement of plant equipment and routing of cable are such that safe shutdown can be achieved with all components (except those protected by 3-hour fire barriers) in any one fire area rendered inoperable by fire.

52 The FPS normally operates in an active standby mode with the fire water supply piping kept full and pressurised. When a fire is detected, the fire detection system produces an audible alarm locally and both visual and audible alarms in the MCR and Security Central Alarm Station. Where the fire area is protected by an automatic suppression system, operation of the suppression system begins. Where the fire area is protected by manual suppression methods, manual fire fighting is the means by which to control and extinguish the fire.

53 Ventilation system fire dampers close automatically against full airflow on high temperature to control the spread of fire and combustion products. Fire dampers serving certain Safety-Related, smoke-sensitive areas are also closed in response to an initiation signal from the Fire Detection System.

54 Fire fighting activities continue until the fire is extinguished. Suppression systems are stopped manually. Operator actions are taken to repair and restore affected detection, alarm and suppression systems to standby status.

2.1.5.4 Conformance with Design Requirements

55 The FPS is classified as a non Safety-Related, non seismic system with the exception of specific seismic design requirements applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following an earthquake and the containment isolation valves and associated piping for the FPS.

56 The FPS is not required to remain functional following a plant accident or the most severe natural phenomena, except for a Safe Shutdown Earthquake (SSE). In addition, the FPS provides a Non-Safety-Related containment spray function.

57 The Fire Protection Analysis (Appendix 9A of the DCD) evaluates the potential for occurrence of fires within the plant and describes how fires are detected and suppressed. It also confirms that the plant can be safely shut down following a postulated fire.

58 The Fire Protection Analysis includes a set of fire area drawings and a discussion of the analysis methodology. It also provides the following information for each fire area in the plant:

- A description of the fire area and its fire barriers, its associated fire zones, as well as fire detection and suppression capabilities.
- Identification of the type, quantity and location of in-situ and anticipated transient combustible materials and combustible loading.
- A listing of Safety-Related mechanical and electrical equipment.
- Fire severity category and equivalent duration.
- An evaluation of FPS adequacy and fire consequences, including a discussion of the control and removal of smoke and hot gases and drainage system adequacy.

59 For fire areas containing Safety-Related structures, systems and components the following information is also provided:

- An evaluation of FPS integrity.
- A safe shutdown evaluation confirming the capability to safely shut down the reactor and maintain it in a safe shutdown condition following a fire.

60 It should be noted that following most fires, non Safety-Related systems are expected to be available to bring the plant to a cold shutdown for repairs. These systems are defence-in-depth systems that are anticipated to be available because of the use of redundant equipment and fire protection features, including separation or automatic fire suppression.

61 If a less likely, more severe fire occurs, these systems are expected to be recovered after reasonable actions are taken to utilise temporary connections or to perform repairs. Recovery of these systems allows the plant to be brought to a cold shutdown for plant repairs. No credit is taken in the fire evaluation for non Safety-Related systems. As a result, fire separation is not required for these systems.

62 Pressure sensors start the fire pumps on decreasing fire main water pressure. Pressure indicators confirm adequate pressures for automatic and manual suppression systems. Valve position sensors are used to monitor the positions of water supply valves.

63 Temperature instrumentation is used to monitor the Fire Water Storage Tank temperature and level instrumentation is used to monitor levels in the Fire Water Storage Tanks and the diesel-driven Fire Pump Fuel Storage Tank.

2.1.5.5 Conformance with Safety Requirements

64 The FPS is considered to have sufficient capacity to fulfil its safety function due to compliance with the applicable regulatory criteria and there are no credible single failures or operator errors that could defeat the performance of the safety function for which the system was designed.

65 The plant layout provides adequate separation between systems to minimise the possibility of a fire in a non Safety-Related system affecting the performance of a Safety-Related system.

66 There is further supporting information relating to the Fire Protection System provided within Chapter 9.5.1 and Appendix A of the DCD.

2.1.6 Toxic / Asphyxiant Gases

67 The AP1000 habitability system is designed to make sure that those areas of the plant for which operator occupancy is desirable for safe operation (although not absolutely necessary, as the passive Safety Measures will cause safe shutdown in the event of an accident) maintain a breathable atmosphere in the event of a toxic or asphyxiant gas release within the plant.

68 Engineered Safety Features (ESFs) protect the public in the event of an accidental release of radioactive fission products from the Reactor Coolant System (RCS). The ESFs function to localise, control, mitigate and terminate such accidents and to maintain radiation exposure levels to the public below applicable limits and guidelines. The habitability system (VES) is included within the PCSR as an ESF.

2.1.6.1 System Safety Functions

69 The VES provides the following Safety-Related functions:

- The VES provides a 72-hour supply of breathable quality air for the occupants of the MCR,
- The VES maintains the MCR pressure boundary at a positive pressure with respect to the surrounding areas. There is a discharge of air through the MCR vestibule,
- The heat loads within the MCR, the Control and Instrumentation (C&I) equipment rooms and the Class 1E dc equipment rooms are within Design Basis assumptions to limit the heat-up of the rooms identified within Chapter 21 of the DCD

2.1.6.2 System Description

70 The VES provides a supply of breathable air for the MCR occupants and maintains the MCR at a positive pressure with respect to the surrounding areas whenever ac power is not available to operate the Nuclear Island Non- Radioactive Ventilation System (VBS) or high radioactivity is detected in the MCR air supply. The VES also limits the heat-up of the MCR, the 1E I&C equipment rooms and the Class 1E dc equipment rooms by using the heat capacity of surrounding structures.

2.1.6.3 Conformance with Safety Requirements

71 A single active failure of a component of the VES does not impair the capability of the systems to accomplish their intended functions.

72 The Class 1E components of the VES are connected to independent Class 1E power supplies.

2.1.7 Explosion

73 The PCSR identifies that explosions could arise due to two sources of initiators, each of which is addressed by means of design justifications or by safety assessments:

- Potential for explosions arising due to combustion of flammable liquids or gases are covered as part of the fire safety assessment,
- Potential for hydrogen explosion is considered within the DCD as a potential source of missiles that could damage the plant. There are several measures addressed via preclusion by design:

i) Batteries present a potential source of hydrogen, so battery compartments are ventilated by a system designed to preclude the possibility of hydrogen accumulation.

ii) Hydrogen supplied to facilities on the nuclear island is stored in a compartment that contains no Safety-Related SSCs. Only one hydrogen bottle at a time is connected to the hydrogen supply line, so the contents of this single bottle represents the maximum potential release – such quantity, even if it remained concentrated in a single compartment (taking no account of ventilation) would not result in an explosion. The hydrogen supply line is not routed through compartments that do not have air movement due to ventilation systems.

iii) The storage area for plant gases is located sufficiently far from the nuclear island that an explosion would not result in missiles more energetic that the tornado missiles for which the nuclear island has designed withstand.

2.1.8 Release of Corrosive Substances

74 Potential for corrosion is considered in the DCD for three potential sources:

- The escape of steam, water, combustible or corrosive fluids, gases, and heat in the event of a pipe rupture will not preclude:
  i) Subsequent access to any areas, as required, to recover from the postulated pipe rupture.
  ii) Habitability of the control room.
  iii) Capability of essential instrumentation, electric power supplies, components, and controls to perform safety functions to the extent necessary to meet the required criteria.
- Prevention of internal pipe and vessel cracking mechanisms potentially involving corrosion (e.g. stress corrosion cracking) is treated implicitly by the plant design via appropriate control of primary coolant chemistry.
- Fire areas are designed to limit the spread of potentially corrosive gases in the event of a fire, with discharge routes to avoid areas where Safety-Related SSCs are located.

2.1.9 Collapsing / Falling Loads

75 The PCSR is limited to providing information relating to the potential for collapsing and falling loads arising from a seismic event.

76 Chapter 9.1 of the DCD provides further detailed information relating to dropped loads and impact associated with the lifting devices included as part of the AP1000 design.

77 Heavy load handling systems consist of equipment which lift loads whose weight is greater than the combined weight of a single spent fuel assembly and its handling device. This equipment is part of the mechanical handling system (MHS) and is located throughout the plant. The heavy load handling systems located in the safety-related areas of the plant, specifically the nuclear island are:

- Containment Polar Crane.
- Equipment Hatch Hoist.
- Maintenance Hatch Hoist.
- Cask Handling Crane.

- MSIV Monorails Hoist A.
- MSIV Monorails Hoist B.

78 For AP1000, a heavy load is a load whose weight is greater than the combined weight of a fuel assembly with rod cluster control, and the associated handling device (≈ 1400 kg).

79 Plant arrangement and the design of heavy load handling systems are based on the following criteria:

- To the extent practicable, heavy loads are not carried over or near safety-related components, including irradiated fuel and safe shutdown components. Safe load paths are designated for heavy load handling in safety-related areas.
- The likelihood of a load drop is extremely small (that is, the handling system is single failure proof), or the consequences of a postulated load drop are within acceptable limits.
- Single-failure-proof systems can stop and hold a critical load following the credible failure of a single component.
- Single-failure-proof systems can support a critical load during and after a safe shutdown earthquake.

80 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. Either redundancy or double design factor is provided for load bearing components such as the hoisting ropes, sheaves, equalizer assembly, hooks, 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.

81 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.

82 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.

83 The heavy loads analysis is to confirm that a postulated load drop does not cause unacceptable damage to reactor fuel elements, or loss of safe shutdown or decay heat removal capability.

2.2 Nuclear Directorate Standards and Criteria

84 The Safety Assessment Principles (SAPs) has been used as the basis for the assessment of the internal hazards associated with AP1000 design. The guidance contained within the SAPs consider that internal hazards on a nuclear power plant or nuclear chemical plant site be identified and addressed in safety assessments. Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous material or gas, flooding etc. which originate within the site boundary, but external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors. The SAPs define internal and external hazards as:

"Internal hazards are those hazards to plant and structures that originate within the site boundary but are, for example, external to the process in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. That is, the duty holder has control over the initiating event in some form. Internal hazards include internal flooding, fire, toxic gas release, dropped loads and explosion/missiles."

85 The guidance within the SAPs consider that the risk from hazards be minimised by attention to plant layout, by keeping inventories of flammable materials and toxic substances to a minimum, and through other good safety management practices. In addition adequate provision against the effects of fire, steam release and missiles affecting safety systems both internal and external to the reactor building and turbine hall should be considered. The key SAPs relevant to the assessment of the Westinghouse AP1000 design are contained within Table 1 of this report.

86 There is additional guidance detailed within ND internal guidance for assessment, specifically the Technical Assessment Guide (TAG) 014 on Internal Hazards (Ref. 8).

87 In addition to internal guidance there is also relevant good practice contained within nuclear specific international guidance that is used as a means to inform the judgment and as a means to assess adequacy of the design e.g. international guidance produced by the International Atomic Energy Agency (IAEA) and the Western European Nuclear Regulators' Association (WENRA) Reference Levels.

2.3 Nuclear Directorate Assessment

88 The approach to the structure of this assessment report for Step 3 was to first confirm, or otherwise, that the observations made during the Step 2 phase of the GDA process had been addressed or adequately captured through further technical queries, regulatory observations or through the continuation of the assessment into Step 4. The outcome of this assessment is contained within Section 2.3.1. Secondly, there was a need to undertake internal hazards assessment on the claims and arguments contained within the PCSR and other supporting documents that had been produced by Westinghouse as part of the safety demonstration for Steps 3 and 4 of the GDA process. This assessment is contained within Section 2.3.2 – 2.3.8 and is concluded within Section 3.

89 It is important to stress that not all areas have been assessed to the same extent due to the sampling nature of the assessment and due to the limited detailed information contained within the PCSR and DCD as there are areas where detailed claims and arguments are yet to be presented.

2.3.1 Assessment of Observations Made During Step 2

90 Ten observations were made within the AP1000 Internal Hazards Assessment carried out for Step 2 of the GDA Process and each of the observations are addressed specifically. At the time these observations were raised a PCSR had not been produced for the AP1000 and as a result the observations were sourced from the Design Control Document (DCD) for AP1000 provided as part of the Step 2 process.

"O1. Information will be required on the methodology used to identify internal hazards."

91 A Technical Query (TQ) (TQ-AP1000-013) (Ref. 10) relating to the internal hazards identification methodology was raised as the means to address this observation. The response to this TQ (Ref. 10) did not identify the methodology applied, it simply made reference to an earlier TQ response (TQ-AP1000-009) (Ref. 10) which related to the completeness of the internal hazards listing. Shortly after these responses were issued

to ND, WEC recognised that the approach taken to the assessment within the US differed significantly from the claims, arguments and evidence approach within the UK. As a result WEC identified the need to produce an Internal Hazards Topic Report (Ref. 11) 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 as a result of TQs that had been raised and closed but which provided answers that were deemed not to adequately address the TQ.

92 The Internal Hazards Topic Report 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 has been identified as requiring assessment within Step 4 as part of the assessment of the Internal Hazards Topic Report.

"*O2. Justification will be required for the completeness of the internal hazard listing".*

93 A TQ (TQ-AP1000-009) (Ref. 10) relating to the completeness of the internal hazards listing within the DCD was raised to address this observation. The TQ response (Ref. 10) was not deemed to adequately respond to the question raised within the TQ, however, subsequent assessment of the PCSR states that the following internal hazards have been considered as part of the AP1000 design:

- Internal Flooding.
- Missile Protection.
- Pipewhip.
- Spray.
- Fire.
- Toxic / Asphyxiant Gases.
- Explosion.
- Release of Corrosive Substance.
- Collapsing / Falling Loads.

94 The internal hazards identified within the PCSR is consistent with the HSE SAPs which states within EHA.14 that, *"Sources that could give rise to fire, explosion, missiles, toxic gas, 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."*

95 I have assessed the information relating to the completeness of the internal hazards listing provided within the PCSR and am satisfied that all the potential internal hazards that could have an impact on nuclear safety have been identified.

"O3. Information will be required on the specific combinations of internal hazards and faults included in the internal hazards analysis."

96 A TQ (TQ-AP1000-014) (Ref. 10) relating to hazard combinations was raised to address this observation. The TQ response (Ref. 10) states that the AP1000 design does not evaluate simultaneous, independent, initiating events. An example of such an event would be a LOCA and a steam line break. The reason for this approach is that the probability of two independent events occurring at the same time is incredibly low, much below a reasonable cut-off frequency. AP1000 does include coincident occurrences that

may be caused by the initiating event. For example, events that result in a reactor trip are also assumed to lose offsite power as a consequence.

97 The AP1000 design does not assume that a component is out for maintenance at the time of an accident and the reason being is that the operability of components is controlled by the plant Technical Specifications. The Technical Specifications are written such that the allowable time a component may be inoperable is dependent on whether the plant can mitigate all Design Basis Accidents (DBAs) with the component inoperable. If the plant can not mitigate against all such DBAs, then there are requirements detailed within these Technical Specifications that require operator action to regain compliance within a short period of time, typically within two hours. In evaluating whether the plant can mitigate DBAs with a component out for maintenance, a single failure is not assumed.

98 I am satisfied with this approach given the statements relating to low frequency of multiple independent faults, consideration of coincidental occurrences as a result of a single internal hazard and the identification that maintenance of plant and equipment is controlled by the use of Technical Specifications is consistent with the practice adopted within the UK reactor fleet.

"O4. Justification will be required for the adequacy of the fire barriers. This should include: a justification of the fire severity and the fire barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control (i.e. minimisation) and design of penetrations."

99 A TQ (TQ-AP1000-0010) (Ref. 10) relating to fire barriers was raised to address this observation. The response to TQ-AP1000-0010 did not adequately address the question being raised, rather it described the principles adopted for fire protection from the DCD. WEC stated that this response addressed a number of TQs. The response did not specifically address the justification of the fire barriers and their associated fire resistance, designation, safety classification and the measures in place to control penetrations. A further TQ (TQ-AP1000-0034) (Ref. 10) was raised repeating the request stated within TQ-AP1000-0010 to which WEC responded by providing information relating to the three hour barriers and the design requirements placed upon those barriers. There were no arguments or evidence presented within the response to the TQ, however, after further discussion, WEC agreed to produce a hazard barrier matrix to compliment the Internal Hazards Topic Report being produced to provide the necessary arguments and evidence to support the fire resistance rating and qualification of the barriers.

100 The responses to both TQ-AP1000-0010 and TQ-AP1000-0034 did not adequately address the technical questions raised. The claims currently made seem reasonable, however, there is a lack of arguments and evidence currently presented within the internal hazards topic report and the hazard barrier matrix has yet to be issued to ND.

"O5. Confirmation will be required that the fire protection system does not perform any safety-related function in ensuring nuclear safety."

101 A TQ (TQ-AP1000-0015) (Ref.10) relating to the nuclear safety claims associated with the Fire Protection System (FPS) was raised to address this observation. The response to the TQ (Ref. 10) stated that this query had been addressed within the response to TQ-AP1000-0010. The response within TQ-AP1000-0010 did not address the query relating to the necessary confirmation that the FPS does not perform a nuclear safety function, however it alludes to the fact that there could be a nuclear safety claim on the fire protection system in some areas to prevent fire spread beyond compartments and as part of the fire influence approach within Containment. Claims on the fire protection system in

this case would result in requirements for the availability and reliability of such a system. Further clarification was sought through the re-issue of this TQ as TQ-AP1000-0037 to which WEC responded by stating, *"The AP1000 has very robust fire protection. The fire protection includes elimination of potential fires by eliminating combustibles and locating combustibles away from safety important components. An example of the first approach is the use of canned motor reactor coolant pumps (RCP). This type of pump eliminates a significant combustible source (lubricating oil) that is used in the type of pump (shaft seal) typically used for RCPs. Use of lubricating oil in RCPs is a significant fire hazard because the surface temperature of the pumps is sufficient to ignite the oil. An example of the second approach is the location of the onsite diesel generators and their fuel oil supply well away from the Auxiliary Building and the Containment Building."* This response had little relevance to the query that had been raised.

102 The responses to both TQs did not address the queries raised, however, 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.

"O6. Justification will be required for any exceptions to the strategy of separating the redundant trains of safety-related equipment with fire/hazard barriers."

103 A TQ (TQ-AP1000-0011) (Ref. 10) relating to exceptions to segregation was raised to address this observation. Once again, WEC stated that the response to this TQ was captured within the response to TQ-AP1000-0010 (Ref. 10), which identifies four areas where segregation has not been achieved and hence exceptions to segregation exist; these areas are the Main Control Room, the area above the Main Control Room, Remote Shutdown Room and Containment. There are a number of claims associated with these areas, however, there is little in the way of arguments provided as part of this response. Further clarification was sought through raising the query again through TQ-AP1000-0035, and the response stated that there were two areas where such exceptions exist, namely the MCR and Containment. There was further clarification of the methodology applied when full segregation was not achievable and this was done through 1 hour barriers coupled with the use of fire suppression and detection systems within those areas, or by 20 feet of physical separation with no intervening combustibles. The response also states that in all areas, other than the MCR and Containment, the arrangement of plant equipment and cable routes are such that safe shutdown can be achieved with all components (except those protected by a 3 hour barrier) in any one fire area rendered inoperable by fire.

104 The use of 1 hour barriers coupled with fire detection and suppression indicates the potential nuclear safety claim associated with ensuring that multiple trains are not rendered inoperable by fire. The query relating to nuclear safety claims associated with the use of a fire protection system have been discussed within the response to Observation 5.

105 The use of a 20 feet separation distance with no intervening combustibles is not recognised within existing UK reactor fleet and nor is it recognised within international relevant good practice stated within IAEA NS.G.1.7 (Ref. 12). The approach to using distance to separate trains of protection is identified as part of the fire influence/fire cell approach, however, the arbitrary distance of 20 feet is not mentioned as the approach that is detailed within the guidance is based upon assessment through a fire hazards analysis to determine what distance is required in order to prevent fire propagation to more than one train of protection. The 20 feet in the case of a fire within containment given there is a limited combustible inventory (as there is no lubricating oil associated

with the Reactor Coolant Pumps) may be reasonable, however, there are currently no arguments to support the application of the 20 feet separation by distance.

106 Both responses to the TQs raised did not provide the requested justification for the areas where there are exceptions to segregation, rather they provided the areas where claims would need to be made but failed to provide adequate detailed arguments to support the claims being made. Further discussions have taken place with WEC and a greater appreciation of the areas where there are exceptions to segregation coupled with the proposed arguments has been realised, however, there is a need for such arguments and evidence to be included within the safety documentation to support the GDA.

"O7. Information will be required on the application of the defence in depth philosophy (prevention, limiting severity and limiting consequences) to internal hazards."

107 A TQ (TQ-AP1000-0016) (Ref. 10) relating to defence in depth was raised to address this observation. The response to the TQ (Ref. 10) provided claims relating to fire and flood and did not address any claims associated with other potential internal hazards. The information which was presented in the response to the TQ for fire and flood was limited and provided examples rather than providing explicit statements of the application of defence in depth. In the case of flooding, the statements made within the TQ response are essentially nuclear safety claims to prevent a flood height sufficient to affect the batteries located within the Auxiliary Building. Likewise the statements made relating to minimising consequences within the Containment and Auxiliary Building are associated with achieving safe shutdown by the use of passive components appear to be nuclear safety claims and not defence in depth.

108 There is a need for further assessment of the statements of defence in depth for all internal hazards within the Step 4 assessment. This is due to the uncertainty and ambiguity within the safety documentation provided by WEC associated with what constitutes a nuclear safety claim and the differences between claims and the principle of defence in depth..

"O8. Information will be required on the layout provisions required to facilitate access for any necessary recovery actions following an event."

109 A TQ (TQ-AP1000-0012) (Ref. 10) relating to minimisation of the effects of incidents was raised as a means to address this observation. The response to this TQ implies, that for events requiring the passive safety-related systems in containment, all necessary post recovery actions can be accomplished within the MCR and there is no need for operator actions outside of the MCR. For the longer term, >72hrs, the response states that some limited actions outside the MCR may be necessary to support the continued operation of the passive safety-related systems. The response does not identify these actions as requested by the TQ, however, the response states that it has been shown that these local manual actions can be performed.

110 Operator actions are to be the subject of detailed assessment within Step 4 as ND are not yet satisfied that operator actions have been considered for less significant but possibly more frequent internal hazards events.

"O9. Justification will be required for the adequacy of the hazard barriers. This should include a justification of the hazard challenge to the barrier, a justification of the hazard barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control (i.e. minimisation) and design of penetrations."

111 A TQ (TQ-AP1000-0018) relating to safety systems and failure independence was raised to address this observation. This TQ was similar to TQ-AP1000-0010, however, the

scope of the TQ was broader to include all internal hazards not just fire. WEC has not previously considered explicit qualification and substantiation of hazard barriers and this TQ resulted in some uncertainty of how to address the issue specifically within the AP1000 safety documentation.

112 It became apparent that the most effective method to address this TQ would be through interaction within Level 4 meetings to determine what provisions were in place relating to claims made on hazard barriers to protect against hazards other than fire and to ensure that these claims were captured within the appropriate safety documentation. Subsequent discussions identified that WEC would not make explicit claims on barriers to provide protection against other internal hazards; the barrier would be adequately designed to protect against them i.e. barriers designed to protect against flooding would not have penetrations through into areas where the potential for flood could have a detrimental effect on the ability of SSCs to perform their required safety function. An example of this is the barrier between the Main Steam Isolation Valve (MSIV) room and the Auxiliary Building – the floors and walls of this room that adjoin the Auxiliary Building are three hour rated for fire, however, there are no penetrations within the barrier as the threat associated with failure of a main feedwater line and the potential for internal flooding was recognised but not explicitly captured within the safety documentation. There are a number of further areas where claims are made implicitly and not captured within the safety documentation.

113 Further to these discussions, WEC identified that the scope of the hazard barrier matrix document could be extended to include claims made on the barriers against other internal hazards not just fire. WEC also recognised the need for the claims, arguments and evidence associated with the effects of all internal hazards on the barriers to be captured within the internal hazards topic report.

"O10. Claims and supporting arguments will be required for the remaining internal hazard and related SAPs, including:

EHA. 3, 4, 7, 10, 13 & 15.

EHF.7

ESR.1 & 6"

114 A TQ was raised (TQ-AP1000-0008) (Ref. 10) relating to claims and arguments to support Step 3 for a number of internal hazards SAPs to address this observation. The TQ response made specific comment against each of the SAPs stated above:

115 *"EHA.3 - 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."* WEC have responded to this SAP by stating that there are a number of areas where the design precludes the potential for an internal hazard occurring e.g. stating that flooding within the Auxiliary Building is prevented as there are no water sources contained within the building. In addition, there are statements associated with the reduction of the potential frequency and severity of RCP fires, and the use of segregation and separation to prevent hazard escalation. Whilst these principles are positive methods of minimising the potential severity and consequences associated with internal hazards, the claims and arguments have not been fully presented within the PCSR. These issues associated with the presentation of the internal hazards safety case culminated in ND issuing a Regulatory Observation (RO.31) (Ref. 13) and associated Regulatory Observation Action (ROA.31) (Ref. 13) was raised. The ROA required WEC 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.

116 *"EHA.4 - 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)".* The response from WEC states that the philosophy associated with internal hazards is to either design out the possibility of a hazard occurring or assume the hazard occurs. There is also the assumption of a 'worst credible' single failure for all design basis faults. In addition, the response states that common mode failures of components have been designed out and the resulting multiple failures would require multiple events to occur simultaneously and are therefore beyond the design basis. This is an acceptable process to adopt, however, the information is based upon the design basis events, therefore, should an event be excluded from the design basis e.g. flooding of the Auxiliary Building, it may not necessarily be captured. As a result the requisite claims, arguments and evidence associated with the SSCs in place to prevent that fault occurring would not be captured also. This has been captured through the RO discussed above.

117 *"EHA.7 - A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences"*. The response provides information relating to the fire Probabilistic Risk Assessment (PRA) and the potential for fires to cause multiple failures and loss of core cooling and states that in order for this to occur, fire barriers must be breached. The outcome being that within the design basis accident analysis assumptions associated with breaches in fire barriers are not permitted. Furthermore, the response states that the fire PRA analysis demonstrates that there are no 'cliff edge' effects with the AP1000 relating to fire protection. This response indicates a high degree of reliability associated with the fire barriers, which has yet to be provided as part of the supporting arguments and evidence. The barriers are currently classed as 'Non-Safety' within the US classification system, which means that they do not have a significant safety claim upon them. This appears to contradict what appears to be a claim that failure of fire barriers is incredible. There is a great deal of operating experience feedback worldwide associated with failures of both active and passive features of nuclear significant hazard barriers and this has been through a number of failures, most notably ageing and degradation and maintenance. Claims, arguments and evidence associated with compliance with this SAP are to be addressed as part of RO.31.

118 *"EHA.10 - The design of facility should include protective measures against the effects of electromagnetic interference (EMI)."* The response states that WEC will place equipment in locations where existing EMI qualification programs have demonstrated both the type and severity of EMI interferences have been accounted for. In addition, it states that EMI will be assessed to identify potential sources and steps taken to ensure that there is adequate testing prior to installation. This area has not yet been subject to any assessment by ND and will be the subject of assessment during Step 4.

119 *"EHA.13 - 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."* WEC responded to this aspect of the TQ within a further TQ response (TQ-AP1000-0041) which attached a WEC document entitled, *"The Applicability of Control of Major Accident Hazards (COMAH) Regulations to AP1000"* (Ref. 14). This document has not been assessed during Step 3 and will be reviewed during Step 4.

120 *"EHA.15 - The design of the facility should prevent water from adversely affecting structures, systems and components important to safety."* The response provides an overview of the case as presented within the DCD. As has already been identified within previous TQ responses there is a need for WEC to adopt a claims, arguments and evidence structure to the safety case. Claims, arguments and evidence associated with compliance with this SAP are to be addressed as part of RO.31.

121 *"EHF.7 - User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states."* The response from WEC considers the fire detection and alarm system, however, there is no mention of any other plant and equipment associated with control, monitoring or indication of potential internal hazards. It is not clear if there is further equipment associated with the internal hazards safety case e.g. level monitoring for internal flooding, H_2 monitoring within battery rooms etc.

122 *"ESR.1 - Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility."* The response, again, only considers fire detection and alarm systems and not other potential safety-related systems associated with internal hazards.

123 *"ESR.6 - Safety-related system control and instrumentation should be operated from power supplies whose reliabilities and availabilities are consistent with the functions being performed."* The response states that there is a Non-Class 1E uninterruptible power supply system that supplies the fire detection and alarm system. It is not clear if there are any plant monitoring systems associated with potential internal hazards other than fire.

2.3.1.1 Conclusions of the Step 2 Observation Assessment

124 There are a number of areas from the Step 2 assessment where further assessment work is required, in part due to the approach taken by WEC to address internal hazards within the PCSR but also in areas where there is a lack of detailed arguments and evidence to support the high level claims. As a result of the process applied to the production of the PCSR and the lack of specific claims, together with the necessary detailed arguments and evidence, a Regulatory Observation (RO) was raised.

125 The Internal Hazards Topic Report is to be assessed in detail within Step 4, as has already been identified from the number of findings associated further assessment.

2.3.2 AP1000 Internal Hazards Topic Report

126 During Step 3, it became apparent that the methodology applied to the presentation of internal hazards safety case documentation was inconsistent with the approach taken within the UK relating to the need to provide detailed claims, arguments and evidence as part of the safety submission. As a result WEC identified the need to produce an Internal Hazards Topic Report (Ref. 11) 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 safety substantiation that focussed on the claims, arguments and evidence structure.

127 Due to the significance associated with the need to provide an adequate safety case for internal hazards a Regulatory Observation (RO.31) and associated Regulatory Observation Action (ROA.31) was raised. The ROA required WEC 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. The means by which WEC proposed addressing the RO was by providing the Internal Hazards Topic Report that included the claims, arguments and evidence required to demonstrate an adequate design for the prevention and control of internal hazards associated with the AP1000 design. It was recognised that there could be a number of iterations of this document as more detailed design information becomes

available relating to the specific evidence required to present the case. WEC proposed that in the first instance and for Step 3 the document would focus on the detailed claims and arguments required to form the basis of the safety case.

128 Initially, the Internal Hazards Topic Report was to be issued to ND in June 2009, however, this date was not achieved and the report was formally issued to ND in August 2009. These timescales were insufficient to undertake a detailed assessment of the content within Step 3 and as a result Sections 2.3.3. through to 2.3.11 of this assessment report has focussed on principles detailed within the PCSR and DCD. In addition to these sources of information, there have been a number of meetings between ND and WEC that have provided additional clarity to the Step 3 internal hazards assessment; some of these areas have yet to be captured within the safety documentation and where this has occurred specific statement has been made within this assessment. Assessment of the Internal Hazards Topic Report has been identified as an assessment task to be undertaken during Step 4.

2.3.3 Nuclear Fire Safety Assessment

129 The focus of the assessment during Step 3 was to identify claims and arguments that, if not adequately conceived, had the potential to result in a significant challenge to nuclear safety as well as result in changes to the design and layout of the AP1000. The buildings that have been assessed specifically were the Auxiliary Building and the Reactor Building, including the Containment structure.

130 No assessment has yet been undertaken on the Fuel Building, the Waste Building, the Fire Fighting Pumphouse or the Turbine Hall.

2.3.3.1 Nuclear Fire Hazard Segregation

131 The principle claim associated with design for fire of the AP1000 is associated with ensuring segregation of the four divisional trains contained within the Auxiliary Building and Containment. The method that has been applied is to provide segregation using fire resistant barriers and enclosures that are designed to withstand fire for a minimum period of three hours. The cable routes have been designed such that there are very few areas where all four trains are located within a common area and in areas where this does exist the cables have been enclosed or separated by distance.

132 A number of meetings have been held between ND and WEC which have provided greater clarity in the design of specific areas in relation to segregation of trains of protection, however, the detailed claims and arguments have not been captured explicitly within the PCSR or the DCD. The PCSR identifies high level claims, however, there is no specific detail with regard to claims made within key areas of the design e.g. in Containment and within the MCR. In addition, there has been no presentation of the arguments and evidence to support the claims that have been made. This concern was raised by ND during Step 3 and as mentioned within Section 2.3.2 WEC identified the need to produce the Internal Hazards Topic Report to address this shortfall.

133 Whilst in principle, the approach is consistent with UK expectations regarding the provision of segregation of SSCs important to safety, assessment of the detailed claims, arguments and evidence will be required during Step 4.

2.3.3.2 Fire Protection Systems

134 Fire Protection Systems (FPS) were also considered during Step 3 with specific focus on nuclear safety claims associated with the provision of the system within the buildings assessed. During Step 2 an observation was made (Observation 5) that was

subsequently converted into two TQs (TQ-AP1000-0015 and TQ-AP1000-0037), which has been addressed within Section 2.3.1 of this assessment report. Further assessment of the PCSR has revealed claims on the FPS as a means to ensure nuclear safety. For example, the PCSR states within Section 5.5.6.5, *"The Fire Protection System (FPS) has been designed to provide expedient fire detection and suppression in line with the nuclear safety implications of fires in specific areas of plant; it has been designed to take consideration of the fire hazard analysis, to make sure that Safety-Related SSCs required for safe plant shutdown or to prevent significant releases of radioactive material can maintain functionality."*

135 IAEA NS.G.1.7 states, *"Where fire detection or extinguishing systems are credited as active elements of a fire cell or fire compartment, arrangements for their design, procurement, installation verification and periodic testing should be sufficiently stringent to ensure their permanent availability. A fire extinguishing system should be included in the assessment against the single failure criterion for the safety function it protects."* Should the FPS be required to provide a nuclear safety function then consideration would need to be given to ensuring availability of such a system e.g. on loss of power, as well as consideration of the integrity and reliability of such a system and the need to take into account single failure. Should the system be classed as "defence in depth", adequate substantiation of the other passive fire protection claims that ensure fire does not result in loss of more than one train of protection would need to be provided.

136 The FPS is also identified as providing an alternate source of water to wet the containment dome or to refill the PCCWST, as well as providing an alternate supply to the RNS heat exchanger further loss of CCS function. This appears to constitute a claim on the FPS to perform a function other than to suppress a fire. This is an acceptable approach to take, however, the PCSR lacks the detailed claims and arguments associated with use of the FPS in this application including the nuclear safety significance associated with the FPS failing to perform this secondary function.

137 As mentioned within Section 2.3.1, 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 a result of the statements made within Section 5.5.6 of the PCSR relating to claims on the FPS, further assessment is to be undertaken as part of the Step 4 assessment.

2.3.3.3 Classification of Fire Protection Plant and Equipment Important to Safety

138 The majority of the SSCs associated with the fire protection design of the AP1000 are classified as 'Non-Safety' under the US classification system. The exceptions to this are the containment isolation valves on the hydrant lines passing from the Auxiliary Building into Containment which are classified as 'Safety' due to their function of isolating containment.

139 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.

140 There is currently a comparison document being produced by WEC to address the differences in the approach to safety categorisation and classification between the US and the UK. The WEC categorisation and classification document that is to be produced early in Step 4 is to be the subject of review as part of the Step 4 internal hazards assessment.

2.3.4 Internal Flooding Assessment

141 Within the PCSR there is a high level claim that the nuclear island is protected against the effects of an internal flood by ensuring that there is sufficient redundancy and segregation of SSCs or that SSCs are located above maximum flood heights.

142 The information within the PCSR relating to internal flooding is limited to stating the general provisions in place e.g. enclosures, barriers, kerbs, drains, and leak detection systems, to prevent flooding of Safety-Related equipment. There is no detailed information which states explicitly where these measures are installed and the nuclear safety significance of such provisions. There is reference to flood protection walls within the PCSR but it is not clear where these barriers are and how such barriers are designed and controlled such that any potential head of flood water cannot have a detrimental effect on the barrier or any of the associated penetrations e.g. cable penetrations, doors and Heating, Ventilation and Air Conditioning (HVAC) systems.

143 Whilst the provisions that are suggested are in line with UK expectations for systems to prevent flooding and to control and isolate any potential flood sources, there are no detailed claims and arguments within the PCSR or the DCD associated with the SSCs that require to be protected against the effects of internal flooding.

2.3.5 Dropped Load and Impact Assessment

144 The PCSR states that AP1000 SSCs are justified against collapsing or falling loads through their seismic qualification which demonstrates that they are located a safe distance from potential dropped loads or designed sufficiently to withstand their impact. This statement indicates a fundamental shortfall in the understanding of the assessment of dropped load and impact. Dropped loads and impact assessment should consider the potential for impact on Safety Related SSCs arising from failures in the control systems of lifting equipment, zoning overrides, dynamic magnification, design, maintenance etc. and not solely relating to the seismic categorisation. The approach taken within the PCSR is merely a restatement of the AP1000 seismic case and provides no claims or arguments to indicate that the lifting equipment is adequately designed to prevent dropped loads or impacts on SSCs. Furthermore, it does not reflect the statements made in DCD chapter 9.1.5 on the Manual Handling System (MHS) which describe the lifting equipment.

145 Section 9.1.5 of the DCD provides detailed information about the safety related areas within which heavy load handling systems are installed as part of the AP1000 design. There are a number of criteria associated with the design and use of lifting equipment within these areas. The lifting equipment is designated as single failure proof, which means that the systems are designed to arrest and hold any load through the use of redundant or the application of increased design factors. Where this principle has been applied, dropped loads have been deemed to be not credible. It should be noted that whilst such an arrangement may be acceptable in the short term, it does not reduce the potential hazard of a dropped load, when brakes are released to make a recovery action, for example, there is no defence in depth. In addition, a heavy loads analysis is not undertaken for critical loads handled by the containment polar crane, cask handling crane, the containment equipment hatch hoist and the containment maintenance hatch hoist due to the unlikely potential for a dropped load. The approach taken to incorporating redundancy and additional design factors is consistent with the approach

applied to minimising the potential for dropped loads within the UK, however, assessment of the potential dropped load hazard would be expected to be considered within the safety case.

146 Where practicable, loads are not carried over or near to safety related components and safe load paths are designated, which again is in line with current UK practice, however, reliance on operator control over movements has the potential to increase the potential for impacts arising from human error. In addition, there is limited information relating to impact other than designation of safe load paths and physical features that prevent movement of the cask handling crane over the spent fuel pool. There is no mention of systems in place for zoning control systems and therefore control of crane movements and the administrative controls will require substantiation.

147 In the case of lifting equipment that is not classed as single failure proof, the criteria state that the consequences of a dropped load are within acceptable limits. This claim has not yet been substantiated and as there are a number of lifting devices that are not classed as single failure proof e.g. the fuel handling machine and the refuelling machine, where a dropped load could have nuclear safety consequences and as a result there is a requirement that the risk associated with dropped loads and impact arising from a failure of such lifting equipment is demonstrated to be As Low As Reasonably Practicable (ALARP).

2.3.6 Missile Generation Assessment

148 The two criteria that have been used as the basis for ensuring protection against the effects of missiles within the AP1000 design are, as with other internal hazards areas, high level principle based statements. The statements associated with prevention of missile impact on Safety-Related SSCs and failure mechanisms resulting in missiles do not provide the requisite detail relating to claims and arguments that I would have expected to be included within the PCSR.

149 The DCD provides further detail relating to the protection that is in place to prevent missile impact on SSCs in place to achieve and ensure safe shutdown, including the elimination, where possible, of potential sources of missiles through equipment selection and through the geographical and physical arrangement of plant and structures.

150 There are a number of design requirements, assumptions and criteria detailed within the DCD, which are consistent with UK expectations when considering the potential missile impacts and the criteria that are to be adopted to minimise the potential for missile impact within the AP1000 design.

151 The DCD details specific areas of the AP1000 that are required to be protected against the effects of internally and externally generated missiles, including, the containment vessel, the reactor coolant pump, the passive core cooling system, the Shield Building, the Containment penetration areas, the Auxiliary Building and the Spent Fuel Pit. The document also provides information relating to the evaluations that are necessary to demonstrate that the high level criteria are satisfied. As part of the work undertaken to evaluate the potential missiles, credible missiles are assessed together with their postulate size, energy and potential trajectory. Analysis is then undertaken on the potential targets and their impact on the ability to achieve and maintain safe shutdown. Finally, loss of the potentially impacted components is assessed together with failure of a single active component.

152 The methodology applied to the design of the AP1000 in relation to missile impact is consistent with that stated within the Technical Assessment Guide (TAG), T/AST/014, for internal hazards which states, *"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." And that, *"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."*.

153 For missiles generated outside containment, the potential for missiles to impact on Safety-Related SSCs has been excluded due to the protection offered either by housings, enclosures or by structural aspects of the buildings themselves. In addition, a claim is made relating to the application of a 2% criterion such that if rotating components are used less than 2% of the time they are excluded from the evaluation. There are also claims relating to retention of fragments should Safety-Related rotating equipment or canned motor pumps fail.

154 There are a number of claims detailed above, however, they are non specific principle based claims that do not have supporting detail or arguments beneath them within the DCD. It is unclear what plant, if any, is claimed, and the requisite substantiation of the SSCs to perform their required safety function, namely the prevention of missile impact upon other Safety-Related SSCs.

155 The potential for consequential effects of hazards i.e. dropped load induced missiles, is mentioned but is dismissed with no substantiation provided which details why the potential for a missile to be generated as a result of such an event is incredible.

156 For missiles generated within Containment, the DCD states that such missiles are deemed to be not credible for very similar reasons cited for missiles outside containment e.g. application of the 2% criterion, structural protection afforded to Safety-Related SSCs and containment of missile fragments within pump housings etc. Again, such high level claims do not provide the requisite information relating to the detailed claims and arguments for individual SSCs that perform a function of protecting Safety-Related SSCs.

157 As with missiles outside of Containment, the potential for consequential effects of hazards i.e. dropped load induced missiles, is mentioned but is dismissed with no substantiation provided which details why the potential for a missile to be generated as a result of such an event is incredible.

158

2.3.7 Internal Explosion Assessment

159 Within the PCSR two sources of potential explosions have been identified; the first arising from the combustion of flammable liquids or gases and the second is associated with the potential for missiles arising from a hydrogen explosion. The PCSR states that the first is detailed within Chapter 9.5 and Appendix 9A of the DCD as part of the fire safety assessment and the second is detailed within Chapter 3.5 of the DCD as part of the missile assessment.

160 The potential for an explosion involving flammable liquids or gases is not considered at any point within Chapter 9.5 or Appendix 9A of the DCD. The only reference to flammable liquids or gases is contained within a compliance table (9.5.1-1) associated with the need to store flammable gases outdoors or in separate buildings, and within the reference section relating to a broad range of NFPA Codes and Standards. This is a significant shortfall given the PCSR makes specific reference to these sections as the source of the claims and arguments associated with the potential for explosions to impact on Safety-Related SSCs.

161 There is limited detail relating to any claims and arguments associated with the potential for explosions arising either from the batteries, the bulk storage of hydrogen, or the gas storage area. Addressing each of these areas specifically:

- Battery Room hydrogen evolution – The DCD recognises that the batteries present a potential source of hydrogen and claims that the vent system is designed to preclude the possibility of hydrogen accumulation. This is potentially a claim on the HVAC system that serves the Battery Rooms and as a result the HVAC system would need to be demonstrated to have sufficient reliability and integrity to ensure that it continues to perform its required nuclear safety function i.e. to ensure that there is no potential for an explosive atmosphere to exist. This specific issue was discussed with WEC specialists who stated that hydrogen evolution is greatest when the batteries are being charged. They explained that battery charger is fed from the same power source as the HVAC system serving the Battery Rooms so should you have a loss of ventilation extract within Battery Room due to loss of power, hydrogen evolution would also be terminated and the potential for a flammable atmosphere is significantly reduced. These claims and arguments do not appear within the PCSR or DCD and the DCD, as currently written appears to place a nuclear safety claim on the HVAC system to prevent the formation of an explosive atmosphere. Should the claim for preventing the formation of an explosive atmosphere be associated with common power feed to both the charger and the HVAC extract, further substantiation of other failure mechanisms associated with the HVAC system that results in continual charging of the batteries would need to be provided.
- Hydrogen supplies to the nuclear island – The potential for a hydrogen explosion within containment is discounted due to claims associated with the amount of hydrogen that could be released as well as the volume within which it could be released not resulting in an explosive atmosphere. Whilst, I accept that by limiting the connection of only one hydrogen bottle to the hydrogen supply pipework it is possible to demonstrate that the amount of hydrogen that could potentially be released into the containment is limited, there is a need to demonstrate that this can be ensured through physical means and that this stipulation is captured to ensure that the safety case remains valid for the lifetime of the plant. The claims appear to be associated with ensuring that a limited amount hydrogen can be introduced coupled with dilution of this limited amount within a single Containment compartment to prevent the formation of an explosive atmosphere.
- Gas storage area – The claim associated with the gas storage area is principally one of spatial segregation which is bounded by tornado missiles. There is no detail relating to specific gas storage, quantities, orientation and location other than to state that it is, *"located sufficiently far from the nuclear island"*. Further substantiation of the claims and arguments made associated with the gas storage are therefore required.

2.3.8 Pipewhip

162 The internal hazards assessment of pipewhip, including jet impingement, undertaken as part of the Step 3 GDA process has been limited to a high level assessment of the main principles detailed within the PCSR. The detailed claims and arguments associated with this area as a result of failures of pipework have not yet been subject to any detailed internal hazards assessment.

163 The PCSR states that there are measures to protect systems that are designated as essential for safe shutdown from the effects of pipewhip associated with pipework that has not been demonstrated to leak before breaking. It is not clear from the PCSR or DCD where these potential vulnerabilities exist and what specific measures are in place to ensure that pipewhip cannot have a detrimental effect on the systems designated essential for safe shutdown.

164 There are detailed high level principles in place to ensure that the maximum physical separation of redundant safety-related components as well as segregation of safety-

related and non safety-related components to ensure that the potential for pipewhip arising from a failure of a non safety-related is minimised. In addition to spatial separation, there are principles associated with physical segregation of redundant safety systems within separate compartments. The methods used to protect against pipewhip in this case are consistent with the approaches taken within the existing UK fleet e.g. distance, barriers and restraints. However, as these statements are largely principle based there is a need for assessment of the claims, arguments and evidence associated with pipewhip.

2.3.9 Spray

165 The internal hazards assessment of spray undertaken as part of the Step 3 GDA process has been limited to a high level assessment of the main principles detailed within the PCSR. The detailed claims and arguments associated with this area as a result of failures of pipework have not yet been subject to any detailed internal hazards assessment.

166 The PCSR states that where there is the potential for spray resulting from failure of pipework that is not classed as leak before break, the systems designated essential for safe shutdown are environmentally qualified to protect against such sprays. There is further information relating to the evaluation of essential systems and components to determine what plant and equipment would require protection. There are assumptions that spray would not damage non-electrical equipment and that they are limited to the compartment of origin. In addition the spray effects associated with the use of the fire protection system are considered and, as with the fire case, the assumption is that all equipment within the compartment of fire origin is lost due to spray.

167 The high level principle claims and assumptions are reasonable and in line with current practice within the UK fleet, however, there is one area that does not appear to have been captured within the PCSR and DCD, namely, sprays of fluids other than water e.g. hydraulic oil. Consideration of consequential flooding as a result of sprays are considered within the internal flooding aspects of the PCSR and DCD. Further assessment of the detailed claims, arguments and evidence associated with sprays and the type of sprays possible is to be undertaken during Step 4.

2.3.10 Toxic and Asphyxiant Gases

168 The potential for toxic and asphyxiant gases is considered within the PCSR and the DCD but only in relation to the Main Control Room Habitability System (VES). There appears to be a claim on the system as it forms part of the Engineered Safety Features (ESFs) in place to protect the public in the event of an accidental release of radioactive fission products from the RCS, however, the PCSR states that this system is *"not absolutely necessary, as the passive Safety Measures will cause safe shutdown in the event of an accident"*.

169 The PCSR and the DCD both detail that this system does perform Safety-Related functions associated with providing 72 hours of breathable air, a positive pressure boundary, and a cooling function to the Class 1E systems to limit heat-up within the MCR, I&C equipment rooms and the Class 1E dc equipment rooms. The DCD provides an overview of the system provisions in order to provide the compressed air supply e.g. bottles, valves, flow sensors etc. and details the classification and function of these components, however, there is no explanation to support whether the system has been adequately designed to ensure a 72 hour supply of air, an assessment of the location of the equipment, and any segregation and redundancy requirements associated with the system. The claims associated with the VES system are currently confusing and appear to be more principle based. There is a need to present the nuclear safety claims

associated with this system together with the supporting arguments and evidence within Step 4 of the GDA.

170 It is not clear whether all toxic and asphyxiant gases have been identified within the PCSR and DCD that could have a detrimental effect on nuclear safety either directly or as a result of any operator actions e.g. the secondary effects of toxic smoke arising from fires on Safety-Related plant and equipment or on the ability of operators to undertake any necessary actions.

2.3.11 Release of Corrosive Substances

171 There has been limited assessment of corrosive substances as part of the Step 3 assessment, other than to gain an overview of the philosophy applied to determine the potential areas where corrosive substances need to be considered. In addition, there is limited information contained within the PCSR and the DCD relating to this potential internal hazard.

172 The potential for corrosive substances affecting access requirements, habitability and essential plant and equipment are all valid areas where the potential hazard requires consideration within the safety case. The other areas mentioned relating to corrosion of pipework is not suited to assessment within this internal hazards area. In addition, the release of corrosive substances as a result of fire is normally dealt with as part of the fire assessment, however, should fire result in a release of a corrosive substance that could have an effect on nuclear safety it already have been captured through the process mentioned previously.

173 There is a need for any claims and their associated arguments and evidence to be captured within the safety case to demonstrate that the potential release of corrosive substances cannot have a detrimental effect on nuclear safety.

3 CONCLUSIONS AND RECOMMENDATIONS

174 The PCSR and DCD for the AP1000 have been presented in a structure that is not in line with the expectations of the UK Regulator. This was identified during Step 3 and WEC committed to produce an Internal Hazards Topic Report whose scope was to present the safety case for internal hazards in a claims, arguments and evidence structure. The Internal Hazards Topic Report has now been issued to ND, however there has been insufficient time prior to the end of Step 3 for a detailed assessment to be undertaken. A number of comments made within this report relating to the requirement for a detailed structured case will need to be either addressed by WEC in the Internal Hazards Topic Report or be scheduled to be addressed elsewhere during Step 4. It is the intention to undertake a detailed assessment of the Internal Hazards Topic Report within Step 4 of the GDA process.

175 It is important to stress that not all areas have been assessed to the same extent due to the sampling nature of the assessment and due to the limited detailed information contained within the PCSR and DCD.

176 I conclude that the safety case provided by the Westinghouse has significant shortfalls. My assessment has identified areas where further work will be required before the safety case can be considered acceptable. I consider that there is a need for WEC to address the concerns relating to the lack of detailed claims and arguments presented during Step 3 coupled with the need to provide sufficient evidence during Step 4 in order to produce an adequate safety case submission for internal hazards. The Internal Hazards Topic Report appears to be the mechanism by which this will be demonstrated, however, this has yet to be assessed in detail by ND.

4 REFERENCES

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

2 *GDA Phase 1 – Steps 3 and 4 Internal Hazards Assessment Strategy.* ND Assessment Report 08/031, Trim Record 2008/591915, HSE, 6/11/2008.

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

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

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

6 *ND BMS, Assessment - Assessment Reports.* AST/003, Issue 2, HSE, October 2003.

7 *ND BMS, Guidance: Assessment Reports.* G/AST/003, Issue 2, HSE, October 2003.

8 *ND BMS, Technical Assessment Guide. Internal Hazards.* T/AST/014, Issue 2, HSE, 13/08/2008.

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

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

11 *AP1000 Internal Hazards Topic Report.* Rev 0, UKP-GW-GLR-001, Westinghouse Electric Company LLC, August 2009.

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

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

14 *Applicability of COMAH [Control of Major Accident and Hazard] Regulations to AP1000.* UKP-GW-GL-037, Rev 0, Westinghouse Electric Company LLC, January 2009.

Table 1

Safety Assessment Principles Relevant to the Internal Hazards Assessment of the AP1000

SAP No.	Assessment Topic / SAP Title
EHA –	External and Internal Hazards
EHA.1	Identification
EHA.3	Design basis events
EHA.4	Frequency of exceedance
EHA.5	Operating conditions
EHA.6	Analysis
EHA.7	Cliff-edge effects
EHA.10	Electromagnetic interference
EHA.13	Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials
EHA.14	Fire, explosion, missiles, toxic gases etc – sources of harm
EHA.15	Fire, explosion, missiles, toxic gases etc – effect of water
EHA.16	Fire, explosion, missiles, toxic gases etc – fire detection and fighting
EKP -	Key Principles
EKP.3	Defence in depth
ELO -	Layout
ELO.4	Minimisation of the effects of incidents
ESS -	Safety Systems
ESS.18	Failure independence
EHF -	Human factors
EHF.7	User interfaces
ESR -	Control and Instrumentation of safety-related systems
ESR.1	Provision in control room and other locations
ESR.6	Power supplies

Annex 1 – Internal Hazards – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None				
Regulatory Observations				
RO-AP1000-031	1 June 2009	Internal Hazards Safety Case Documentation	Internal Hazards Topic Report issued to NII 13th August 2009. Report to be assessed by ND during Step 4.	Step 4