HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

GDA Phase 1 - Step 2 WEC – AP1000 Internal Hazard Assessment

HM Nuclear Installations Inspectorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

1. INTRODUCTION

This assessment report records the Step 2 Internal Hazards assessment of the Westinghouse AP1000 submission in accordance with the strategy outlined in the Unit 6D operating plan, Ref 2.

Overall, it was concluded that the WEC claims against the key Internal Hazard Safety Assessment Principles (SAPs) used in Step 2, were reasonable. Supporting arguments and evidence will be required, during Steps 3 & 4, to ensure that the AP1000 design complies with the claims and also complies, where reasonably practicable, with the full range of Internal Hazard SAPs.

In preparation for Step 3 the assessment made a number of observations which identified further information to be provided by WEC in support of the claims.

2. ND ASSESSMENT

A proposal to licence new nuclear power stations in the UK is subjected to a two phase process as detailed in the Generic Design Assessment (GDA) – Guidance to Requesting Parties document, Ref 1. Phase 1 consists of 4 Steps and leads to the issuing of a Design Acceptance Confirmation. A Design Acceptance Confirmation means that the station design will be suitable for construction in the UK subject to a site specific licence being granted at the completion of Phase 2.

This assessment report covers the Internal Hazard assessment carried out in Phase 1, Step 2. Phase 1, Step 2 of the GDA is called the "Fundamental Safety Overview" and covers an overview of the fundamental acceptability of the proposed design concept within the UK regulatory regime, Ref 1.

The overall assessment strategy for Step 2 is defined in the Unit 6D Operating Plan, Ref 2, and the specific Internal Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07010, Ref 3.

As stated in the BMS guidance covering the NII assessment process, G/AST/001, Ref 4, "…..for a safety case to be effective it must provide three elements: *Claims, Evidence and Argument.*" The GDA addresses these elements in a stepwise approach. Phase 1, Step 2 addresses the claims. Phase 1, Step 3 addresses the arguments and Phase 1, Step 4 addresses the evidence. The completion of these Steps in Phase 1 constitutes the completion of the NII assessment covering the generic design and would lead to the issuing of the Design Acceptance Confirmation referred to above.

The objective of this assessment is therefore to consider whether Westinghouse (WEC) claim that the relevant Internal Hazard SAPs are met.

Assessment during Steps 3 & 4 will address the adequacy of the arguments and evidence supporting these claims respectively.

2.1 Requesting Parties Case

The WEC Step 2 submission used during the assessment was located at S:\New Reactor Build\RP Submission\Westinghouse Submission – Sep 2007. The submission was entitled, "UK AP1000 Design Acceptance Application" (Ref 5).

Within the submission, WEC document, "UK Compliance Document for AP1000 Design, Section C – Safety Assessment Principles Roadmap for AP1000 Design", Ref 6, presented a claim of compliance and a discussion on how the AP1000 design addressed each of the principles in the HSE Safety Assessment Principles for Nuclear Facilities, Ref 7, and included cross references to WEC document "UK AP1000 Safety, Security and Environmental Report" (SSER), Ref 8, which contained additional information supporting compliance with the SAPs.

WEC claim that the AP1000 has addressed all relevant UK Safety Assessment Principles. In the context of internal hazards, it is noted that WEC claim to have addressed all of the Internal Hazard SAPs.

2.2 Standards and Criteria

The assessment is conducted in accordance with ND BMS procedures, AST/001, AST/002 and AST/003, Refs 9–11 respectively, and informed by the guidance given in the Internal Hazards Technical Assessment Guide (TAG) T/AST/014, Ref 12.

The Internal Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07010, Ref 3. In accordance with this strategy, the Hazard SAPs, EHA.1 – EHA.17, Ref 7, were reviewed to identify key Internal Hazard SAPs that were relevant to the Step 2 assessment. To ensure that this selection covered an adequate set of Internal Hazard SAPs a further review was carried out against the WENRA reference levels, Ref 13, and the IAEA Nuclear Power Plant Design Requirements, Ref 14. The results of this review are shown in Annex 2 of the Internal Hazards assessment strategy, Ref 3, where they are ordered under assessment topics. These key Internal Hazard SAPs were used during the assessment.

2.3 ND Assessment

The definition of internal hazards is given in Ref 12, it states that, *"Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous materials 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".* This definition was used in the assessment.

The key internal hazard assessment topics addressed in the assessment, as identified in the process described above, were:

- **Internal Hazards**
    - Identification
    - Operating Conditions
    - Analysis
    - Sources of Harm
    - Fire Detection and Fighting
    - Use of Material
- **Defence in Depth**
- **Layout**
    - Effects of Incidents
- **Safety Systems**
    - Failure Independence

The overall objective of these principles is to minimise the effects of internal hazards, particularly to ensure that internal hazards do not adversely affect the reliability of safety systems designed to perform essential safety functions and that the potential common cause effects of internal hazards have been adequately addressed. Safety systems and

safety related systems should be either qualified to withstand the effects of internal hazards or protected against the hazards, i.e. appropriate use of equipment qualification, redundancy, diversity, separation or segregation.

In achieving this objective, the principles require that a comprehensive and systematic approach is used to identify the internal hazards and that the hazards are then appropriately combined with consequential and/or simultaneous hazards and/or faults and, where necessary, take into account plant out for maintenance. A “defence in depth” approach should also be applied to internal hazards, for internal hazards that cannot be eliminated the following approach is used:

- Prevent the hazard
- Limit the severity of the hazard should it occur
- Limit the consequence of the hazard should it occur and be severe

The Step 2 assessment considered whether WEC claimed that each key Internal Hazard SAP had been satisfied. The adequacy of any claim will be judged during Steps 3 & 4 where the arguments and supporting evidence will be assessed. The assessment findings against the key Internal Hazard SAPs are presented in tabular form in Appendix 1. A summary, highlighting a number of observations to be considered during Step 3, is given below and should be read in conjunction with Appendix 1.

2.3.1 Internal hazards

WEC claim that the AP1000 design has addressed these SAPs, Ref 6.

In the response, Ref 6, WEC referred to the following internal hazards: internal flood, missiles, pipe break and fire and included cross references to the SSER for further details on how each hazard was to be addressed within the design. WEC provide limited information on the methodology used to identify the hazards. Consequently, in Step 2, it is not possible to confirm the completeness of the hazard listing.

Whilst WEC claim compliance with SAPs EHA.1 & 14, supporting arguments will be required, during Step 3, to justify their claim and in particular the completeness of the hazard listing. The adequacy of the hazard identification methodology used will need to be assessed during Step 3 and tested using the additional hazards listed in Appendix 1 – EHA.1 & 14.

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

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

In claiming compliance with the SAP requirements for the hazard analysis to include appropriate combinations of consequential and independent hazards and/or faults, WEC refer to compliance with the “General Design Criteria” from USNRC 10 CFR 50, Appendix A, specifically, the hazard related criteria 2, 3 & 4 which relate to natural phenomena, fire

protection and missiles respectively. The USNRC criterion relating to natural phenomena (an external hazard) does contain a requirement for the design to reflect an appropriate combination of the external hazard with normal and accident conditions. However, it is not clear if similar requirements exist in those criteria covering the internal hazards.

Whilst WEC claim compliance with EHA.5 & 6, supporting arguments will be required, during Step 3, to justify their claim and in particular that the AP1000 design has adequately addressed the hazard combination requirements in EHA.5 & 6.

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

WEC claim to provide fire detection and fire fighting systems of appropriate capacity and capability and refer to compliance with USNRC 10 CFR 50, Appendix A, Criterion 3 “Fire Protection”. WEC state that the fire protection system (detection & fire fighting) is a non safety related system. It is noted that the design strategy outside primary containment is to separate the redundant trains of safety-related equipment with 3 hour fire barriers. In containment the design strategy is to use a combination of structural walls, local fire barriers and distance. The WEC claim also referred to a fire hazards analysis which addressed fire prevention, provision of fire barriers and the separation of structures, systems and components important to safety.

The fire resistance of safety related fire barriers is pre-defined, typically 3 hours. The adequacy of this fire rating is dependent on the combustibles in the fire compartments and the resulting fire severity. A justification for the fire resistance of the fire barriers is required.

Whilst WEC claim compliance with SAP EHA.16, supporting arguments will be required, during Step 3, to justify their claim and in particular the adequacy of the fire barriers and any exceptions to the separation strategy.

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.

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

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

2.3.2 Defence in Depth

WEC claim that the AP1000 design is based on the principle of defence in depth and uses the “three traditional levels”:

- Prevention of deviation from normal operation
- Detection of deviation from normal operation and provision of means to prevent such deviations leading to accident conditions
- Provisions of engineering safety features to control and mitigate the accident conditions

It is noted that WEC statements covering a number of internal hazards imply that the defence in depth philosophy is applied to the control and mitigation of internal hazards, most notably the fire hazard.

Whilst WEC claim compliance with SAP EKP.3, supporting arguments will be required, during Step 3, to justify their claim and in particular the application of the defence in depth philosophy to all of the internal hazards.

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

2.3.3 Layout

WEC claim that the effects of internal hazards are minimised and refer to the design provisions for the protection of each internal hazard, including the provisions for accessibility and emergency lighting. The scope of the claims is consistent with the scope of SAP ELO.4 which covers the provisions required to support access for any recovery actions following an event

Whilst WEC claim compliance with SAP ELO.4, supporting arguments will be required, during Step 3, to justify their claim.

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

2.3.4 Safety Systems

One of the requirements in SAP ESS.18 is to ensure that no internal hazard should disable a safety system. WEC claim that the AP1000 has been designed such that the safety systems have adequate separation, redundancy, diversity and protection, so that following an internal hazard the required safety functions are assured.

The separation and protection provisions claimed relate to the use of fire barriers and equipment qualification. The adequacy of these provisions is dependent upon the identification of all appropriate internal hazards. The reference to the term “fire barriers” is not fully descriptive as these passive barriers act as a hazard barrier and will therefore have performance criteria based on the hazard challenge specific to their location, i.e. flood levels, missile impact, overpressure, fire severity, environmental effects etc.

Whilst WEC claim compliance with the internal hazard aspects of SAP ESS.18, supporting arguments will be required, during Step 3, to justify their claim and in particular the adequacy of the hazard barriers. This requirement is linked to the identification of internal hazards which has been discussed above, and the specification of the hazard challenge to each barrier or the equipment qualification.

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.

2.3.5 General

The scope of the Step 2 assessment is limited to the key Internal Hazard SAPs. During Step 3 the full scope of the internal hazard and related SAPs will be assessed. Consequently, claims and supporting arguments will be required for the following SAPs:

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

3. CONCLUSION

The Step 2 Internal Hazards assessment of the AP1000 was completed. The assessment in Step 2 considered the claims made by WEC against each of the key Internal Hazard SAPs.

It was concluded that WEC had made a claim against each key Internal Hazard SAP and as a consequence had met the assessment requirements of Step 2, Ref 2.

Whilst the claims were judged to be reasonable, supporting arguments and evidence will be required, during Steps 3 and 4, to confirm compliance with the claims and also to justify compliance, where reasonably practicable, with the full range of Internal Hazard SAPs. On that basis, I have no objection to the AP1000 proceeding to Step 3.

In preparation for Step 3 the assessment made a number of observations which identified further information to be provided by WEC in support of the claims.

4. RECOMMENDATION

1. It is recommended that the observations identified throughout the assessment report should be raised with WEC during Step 3.

5. REFERENCES

1. HSE Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, Version 2, 16 July 2007.
2. HSE ND DIV 6 Unit 6D Operating Plan, 2 August 2007 – 31 March 2008.
3. HSE ND DIV 6 Assessment Report “GDA Phase 1 - Step 2 Internal Hazards Assessment Strategy”, Assessment Report No AR07010.
4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
5. Westinghouse AP1000, “UK AP1000 Design Acceptance Application”, UKP-GW-GL-710, Revision 0.
6. Westinghouse AP1000, “UK Compliance Document for AP1000 Design, Section C, Safety Assessment Principles Roadmap for AP1000 Design”, UKP-GW-GL-710, Revision 0, Section C.
7. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
8. Westinghouse AP1000, “UK AP1000 Safety, Security and Environmental Report”, UKP-GW-GL-700, Revision 1.
9. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.
10. HSE ND – BMS AST/002, “Assessment - Assessment Activity management”, Issue 003, 16 April 2002.
11. HSE, ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.
12. HSE ND – BMS, “Technical Assessment Guide – Internal Hazards”, T/AST/014, Issue 001, 24 June 1999.
13. Western European Nuclear Regulators Association (WENRA) Reactor Safety Reference Levels, January 2007.
14. IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements – No.NS-R-1.

APPENDIX 1

Assessment of Internal Hazard SAPs Considered During Step 2

Assessment Topic/SAP	Assessment
EXTERNAL AND INTERNAL HAZARDS	
Identification. *Principle EHA.1 - External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.* *Guidance – SAP paragraphs 211-213.* *211 This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.* *212 Any generic type of hazard with a total frequency that is demonstrably below once in ten million years may be excluded. Any generic type of hazard, the impact of which has no effect on the safety of the facility, can also be excluded. This screening should retain all hazards for which the frequency of realisation and the potential impact might make a significant contribution to the overall risks from the facility.* *213 The potential of a hazard to affect the safety of a facility may take account of factors such as the source of the hazard in relation to the facility and the design characteristics of the facility.*	WEC claim that the AP1000 design has addressed this principle. The WEC statement supporting this claim referred to several internal hazards, including internal flood, missiles, pipe breaks and fire and confirmed that internal hazards had been considered in the AP1000 design. The adequacy of the supporting argument and evidence in justifying compliance with EHA.1 will need to be assessed during Steps 3 & 4. This assessment will need to consider the adequacy of the internal hazard identification process in identifying all credible internal hazards and should also include consideration of the following additional internal hazards: • Internal flooding arising from human error. • Spray effects from other than pipe failure, i.e. tanks, fire suppression systems, pump mechanical seals etc. • High trajectory missiles arising from TG disintegration. • Missile arising from pipe breaks. • On-site transport. • Toxic and hazardous substances. • Overpressure from fires. • Dropped loads.
Operating conditions *Principle EHA.5 - Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.*	WEC claim that the AP1000 design has addressed this principle. The scope of principle EHA.5 is intended to cover both internal and external hazards. It is noted that the WEC statement supporting the claim is limited in its scope as it only refers to “natural phenomena”, which forms part of the external hazards area. Consequently, the adequacy of the supporting argument and evidence in justifying compliance with the full scope of EHA.5, particularly internal hazards, will need to be assessed during Steps 3 & 4.
Analysis *Principle EHA.6 - Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.* *Guidance – SAP paragraph 217.* *217 To achieve the above two [EHA 5 & 6] principles the analysis should take into account that:* *a) certain internal or external hazards may not be independent of each other and may occur simultaneously or in a combination that it is reasonable to expect;* *b) an internal or external hazard may occur simultaneously with a facility fault, or when*	WEC claim that the AP1000 design has addressed this principle. WEC’s statement supporting this claim refers to compliance with a number of criteria in USNRC 10 CFR 50, Appendix A, including the hazard related criteria 2, 3 & 4 which relate to natural phenomena, fire protection and missiles respectively. Criterion 2 includes the statement that the design shall, amongst other requirements, reflect appropriate combinations of the effect of normal and accident conditions with the effects of natural phenomena. It is not clear if similar requirements covering appropriate combinations of internal hazards are adequately covered within the other criteria. The adequacy of the supporting argument and evidence in justifying compliance with EHA.6 will need to be assessed during Steps 3 & 4, with particular attention to appropriate combinations of internal hazards and faults in the analysis.

Assessment Topic/SAP	Assessment
plant is out for maintenance; *c) there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;* *d) many internal and external hazards have the potential to threaten more than one level of defence in depth at once;* *e) internal hazards (e.g. fire) can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences; and* *f) the severity of the effects of the internal or external hazard experienced by the facility may be affected by facility layout, interaction, and building size and shape.*	
Fire, explosion, missiles, toxic gases etc – sources of harm *Principle EHA.14 – Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.* *Guidance – SAP paragraph 230.* *230 This identification should take into account:* *a) projects and planned future developments on and off the site;* *b) the adequacy of protection of the nuclear facility from the effects of any incident in an installation, means of transport, pipeline, power supplies, water supplies etc either inside or outside the nuclear site.* *c) sources could be either on or off the site;*	WEC claim that the AP1000 design has addressed this principle. WEC's statement supporting this claim explicitly refers to the internal hazards specified in principle EHA.14, i.e. fire, explosion, missiles, toxic gas release, collapsing or falling loads (i.e. dropped loads), pipe failures and flooding. HSE guidance covering the application of EHA.14 is given in SAP paragraph 230. It is noted that this paragraph increases the scope of EHA.14 with reference to incidents arising from on-site transport, on-site pipelines and on-site power and water supplies. WEC's statement does not make an explicit reference to these potential hazards. Consequently, the adequacy of the supporting argument and evidence in justifying compliance with EHA.14, including the guidance, will need to be assessed during Steps 3 & 4.
Fire, explosion, missiles, toxic gases etc – fire detection and fighting *Principle EHA.16 – Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.* *Guidance – SAP paragraphs 232-233.* *232 The systems should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the facility.* *233 A fire hazard analysis should be made of the facility*	WEC claim that the AP1000 design has addressed this principle. WEC's statement supporting this claim refers to compliance with USNRC 10 CFR 50, Appendix A, Criterion 3 "Fire Protection" which, among other requirements, requires the provision of fire detection and fighting systems of appropriate capacity and capability. WEC's statement also refers to a fire hazards analysis that addresses the broader provisions of a fire protection programme which includes fire prevention, provision of fire barriers and the segregation of SSCs important to safety. The adequacy of the supporting argument and evidence in justifying compliance with EHA.16 will need to be assessed during Steps 3 & 4, with particular attention to the: • Safety categorisation and classification of hazard barriers.

Assessment Topic/SAP	Assessment
to: *a) analyse the potential for fire initiation and growth and the possible consequences on safety systems and other structures, systems and components important to safety;* *b) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire; and* *c) determine the capacity and capability of the detection and fire-fighting systems to be provided.*	• Single failure tolerance of active penetrations in the hazard barriers, where appropriate. • Justification of hazard barrier fire resistance. • Compliance with the relevant good practice established in the IAEA Safety Guide NS-G-1.7 "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants."
Fire, explosion, missiles, toxic gases etc – use of material *Principle EHA.17 - Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.*	WEC claim that the AP1000 design has addressed this principle. WEC's statement supporting this claim refers to compliance with USNRC 10 CFR 50, Appendix A, Criterion 3 "Fire Protection" which, among other requirements, requires the use of non-combustible and heat resistant material wherever practical. The adequacy of the supporting argument and evidence in justifying compliance with EHA.17 will need to be assessed during Steps 3 & 4, with particular attention to the definition and standards used to determine non-combustibility.
KEY PRINCIPLES	
Defence in depth *Principle EKP.3 - A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.* *Guidance – SAP paragraphs 140-144 & Table 1 (not included)* *140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.* *141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation.* *142 The concept of defence in depth should be applied so that:* *a) deviations from normal operation and failures of structures, systems and components important to safety are prevented;* *b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation;*	WEC claim that the AP1000 design has addressed this principle. WEC's state that: *"The basic AP1000 safety philosophy is based on the well-established principle of defence-in-depth. The three traditional levels are:* • *Prevention of deviation from normal operation* • *Detection of deviation from normal operation and provision of means to prevent such deviations leading to accident conditions* • *Provisions of engineering safety features to control and mitigate the accident conditions* *In addition, the prevention and mitigation of severe accident conditions is considered through the development and use of the PRA and supporting analyses results."* The defence in depth philosophy can also be applied to internal hazards, that is: • Prevent the internal hazard. • Limit the severity of the internal hazard. • Limit the consequences of the internal hazard. WEC statements in a number of internal hazard analyses apply this defence in depth philosophy to the control and mitigation of internal hazards, most notably the fire hazard. The adequacy of the supporting argument and evidence in justifying compliance with EKP.3 will need to be assessed during Steps 3 & 4.

Assessment Topic/SAP	Assessment
c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents; *d) additional measures are provided to mitigate the consequences of severe accidents.* *143 Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-1, on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.* *144 An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.*	
LAYOUT	
Minimisation of the effects of incidents *Principle ELO.4 - The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.* *Guidance – SAP paragraphs 206-207.* *206 For example, the design and layout should:* *a) minimise the direct effects of incidents, particularly internal and external hazards, on structures, systems or components;* *b) minimise any interactions between a failed structure, system or component and other safety-related structures, systems or components;* *c) ensure site personnel are physically protected from direct or indirect effects of incidents;* *d) facilitate access for necessary recovery actions following an event.* *207 Support facilities and services important to the safe operation of the nuclear facility should be designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will*	WEC claim that the AP1000 design has addressed this principle. WEC's response refers to the internal hazard provisions covering internal flooding, missiles, pipe break and fire. The overall approach is to prevent the hazards and to minimise the consequences should they occur. Mitigation outside containment is primarily based on the physical separation of redundant safety related components and systems from each other and from non safety related components. Mitigation inside containment is primarily based on appropriate separation by distance and qualification. The adequacy of the supporting argument and evidence in justifying compliance with ELO.4 will need to be assessed during Steps 3 & 4.

Assessment Topic/SAP	Assessment
remain. Support facilities and services include access roads, water supplies, fire mains and site communications.	
SAFETY SYSTEMS	
Failure Independence *Principle ESS.18 - No fault, internal or external hazard should disable a safety system.* *Guidance – SAP paragraph 352.* *352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.*	WEC claim that the AP1000 design has addressed this principle. WEC claim that the AP1000 has been designed such that the safety systems have adequate separation, redundancy, diversity and protection so that required safety functions cannot be disabled by internal hazards. The adequacy of the supporting argument and evidence in justifying compliance with ESS.18 will need to be assessed during Steps 3 & 4.