HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

Step 2 WEC – AP1000 Civil Engineering and External Hazard Assessment

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

1. INTRODUCTION

This assessment report records the Step 2 Siting, Civil Engineering and External Hazards assessment of the Westinghouse (WEC) AP1000 submission in accordance with the strategy outlined in Ref 2.

Overall, it was concluded that the WEC claims against the key Siting, Civil Engineering and External Hazard SAPs used for Step 2, were reasonable. However, 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 Siting, Civil Engineering and External 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 Siting, External Hazards and Civil Engineering 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 Civil Engineering and External Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07007, 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 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 Civil Engineering and External Hazard SAPs are met.

In addition, an overview of the "Generic Site" claims is provided, and a high level overview of the nature of the design from a CDM regulations perspective.

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 is entitled, "UK AP1000 Safety and Environmental Report" (SER).

Within the submission, WEC document, "UK Compliance Document for AP1000 Design", Ref 5, presented a discussion on how the AP1000 design addressed each of the principles in the HSE Safety Assessment Principles for Nuclear Facilities, Ref 6, and included cross references to the SER which contain additional discussions on how the UK safety Assessment Principles (SAPs) were addressed.

WEC claim that the AP1000 has addressed all relevant SAPs in the context of Siting, External Hazards and Civil Engineering.

2.2 Standards and Criteria

The assessment is conducted in accordance with ND BMS procedures, AST/001, AST/002 and AST/003, Refs 7–9 respectively, and informed by the guidance given in the External Hazard, Civil Engineering and Reactor Containment Technical Assessment Guides Ref 10,11 and 12.

The Siting, External Hazards and Civil Engineering assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07007, Ref 3. In accordance with this strategy, the relevant SAPs, were reviewed to identify those key to the Step 2 assessment of Siting, Civil Engineering and External Hazards. To ensure that this selection covered an adequate set of 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 Siting, Civil Engineering and External Hazards assessment strategy, Ref 3, where they are ordered under assessment topic areas.

2.3 ND Assessment

The assessment of Siting, External Hazards and Civil Engineering is by necessity linked, as it is the holistic nature of their consideration which is important. The overall impression formed is that the studies into the following aspects have been undertaken.

- Safety Classification
- Design Standards
- Hazard Identification
- Hazard Quantification
- Siting Envelope Considerations

The depth and breadth of these has not been established in detail, this is a task for Step's 3 and 4.

2.3.1 Siting

WEC claim that the AP1000 design has addressed these SAPs, Ref 5. The compliance document signposts to the external hazards that have been considered directly in the design basis of the plant, and also provides a synopsis of those hazards, which will be considered as part of the site licence application. The approach adopted is reasonable at the Step 2 stage, however a more considered view over the application into the UK situation will be required at the Step 3 assessment, and for the Step 4 considerable attention will be required in this area. Figure 1 in this report shows a basic comparison of the seismic design basis for the AP1000 as compared against a selection of 4 UK sites. As can be seen, it is not apparent that the design envelopes all sites from this simple comparison.

One aspect which has not been addressed is that of population demographics around the installation. This is not a direct requirement of the SAPs other than within certain targets (ie Target 9), where there is a need to examine the impact on the population around a site. It is noted that specific reference is made to the NRC requirements, which define an exclusion zone and a low population zone, and associated limits on radiation exposure. WEC should also be aware that there is a UK Government Policy on the control of Demographics around Nuclear Power Installations. As part of the ongoing Strategic Siting Assessment being undertaken by BERR, this issue is being considered further.

Observation 1 *WEC need to better understand the siting Policy requirements for UK reactors*

Observation 2 *The design criteria have been clearly laid out, however there is no attempt to rationalise the application to the UK, either by inclusion or exclusion of areas/sites*

2.3.2 Civil Engineering

WEC claim that the AP1000 design has addressed these SAPs, Ref 5. There is a safety classification system in place with associated design standards. The design standards are primarily American in nature, and appear where necessary to be specific to Nuclear grade structures. It is noted that some of the standards are now superseded. This aspect will be more carefully examined in Steps 3 and 4, along with a more thorough review of the derivation of the design basis events.

One aspect which does not appear to have been recognised is the use of non US materials for construction in the UK. Whilst this is not seen as a major impediment, the increased globalisation of the supply chain means that the translation of the requirements to more generic basis will be essential.

Observation 3 *Clarity over the design classification for structures will need to be provided. It is recognised that the 10CFR 50 approach has been adopted, however, its interpretation into UK expectations is still needed. The links from design classification to design standards will need further investigation to ensure that the intent is satisfied.*

Observation 4 *The standards used need to be understood better, especially where they are not international. In addition, it is noted that a number of now superseded standards have been used. In particular ACI 349-01, which has now been superseded by ACI 349-06, and ANSI/AISC N690-94 which has been superseded by and ANSI/AISC N690L-03.*

Observation 5 *There needs to be a recognition that non-US spec materials will be used for construction*

Within the DCD, there is a detailed description of the design criteria applied to the founding materials for the AP1000 standard design. These are expressed as a limiting value for the static allowable bearing pressure of 8600lb/ft2 and a shear wave velocity of the founding material of greater than 1000 ft/sec. A brief review of current UK Nuclear power coastal sites has shown that there are a number, which may not satisfy this criteria. This is primarily in sites where there is a significant depth of alluvium or post glacial deposits.

Observation 6 *The limiting allowable bearing capacity is stated as 8600lb/ft^2. This value may limit the number of available sites in the UK.*

Observation 7 *The minimum shear wave velocity required is stated as 1000ft/sec. There are a number of existing sites where this value will not be reached, where for example; there is deep alluvium or shingle.*

2.3.3 External Hazards

WEC claim that the AP1000 design has addressed these SAPs, Ref 5. The documents supplied provide a clear statement over the design conditions applied to the plant and in addition identify those aspects which will require further consideration once a site or sites have been identified. The range of hazards considered is seen as reasonable, however there does not appear to be a consideration of lightning as an external hazard. In addition, there is no specific recognition of climate change as a driver for a number of hazards. The current list of hazards recognises that some cannot be defined until a site (or sites) have been defined. For other hazards, limiting values are provided. It is claimed that consequential or secondary hazards are considered in the design process. The process for this will require greater scrutiny in Step 3

Observation 8 *The process for Hazards ID, definition and consideration of consequential effects will require greater scrutiny in Step 3. The definitions of coincident plant states with hazards will also be reviewed in detail; consideration of consequential effects will require greater scrutiny in Step 3.*

Observation 9 *The list of external hazards identified in the Site Characteristics Document does not fully recognise the extent of hazards which will need to be considered as part of the final design*

One of the requirements in SAP ESS.18 is to ensure that no external 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 the required safety functions cannot be disabled by external hazards. This claim works for some hazards, however for others such as flood, wind and seismic, the effects are similar to all areas of the plant. A more considered view of this will be required.

Observation 10 *A more considered view of the claims against ESS.18 ("no external hazard should disable a safety system"), including the link to the PRA will be required. This will also include a review of "Cliff edge" considerations.*

A Technical Query (TQ) on the subject of Directed Aircraft Impact (TQ AP1000-000006) was raised with WEC, and they have responded. This has confirmed that the design has considered the effects of aircraft impact of a malicious nature. These claims will be considered in more detail in Step 3.

2.3.4 CDM Regulations

There is no specific mention of the Construction Design and Management Regulations 2007 (CDM) located in any of the submissions reviewed to date. This is unsurprising, as they have been primarily designed for submission to the USNRC, which does not have such a requirement.

Observation 11 *There needs to be a recognition that the Construction Design and Management Regulations 2007 will apply to this project*

3. CONCLUSION

Westinghouse claim compliance with the key Siting, External Hazards and Civil Engineering SAPs in Appendix 1.

Overall, it was concluded that the claims made by WEC, against the key SAPs used for Step 2, were reasonable. However, supporting arguments and evidence will be required, during Steps 3 & 4, to ensure that the AP1000 design complies with the claims

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. The observations identified throughout this assessment report will require a response from Westinghouse 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 “Step 2 External Hazards Assessment Strategy”, Assessment Report No 2007/07.
4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
5. Westinghouse AP1000, “UK Compliance Document for AP1000 Design, Section C, Safety Assessment Principles Roadmap for AP1000 Design”, UKP-GW-GL-710, Revision 0.
6. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.
7. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.
8. HSE ND – BMS AST/002, “Assessment - Assessment Activity management”, Issue 003, 16 April 2002.
9. HSE ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.
10. HSE ND – BMS, “Technical Assessment Guide – External Hazards”, T/AST/013, Issue 002, 24 Jan 2005
11. HSE ND – BMS, “Technical Assessment Guide – Structural Integrity Civil Engineering Aspects”, T/AST/017, Issue 002, 17 March 2005
12. HSE ND – BMS, “Technical Assessment Guide – Containment for Reactor Plant”, T/AST/020, Issue 001, 25 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 Civil Engineering and External Hazard SAPs Considered During Step 2

Assessment Topic/SAP	Assessment
Safety classification and standards	
Safety categorisation *Principle ECS.1 - The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.* *Guidance - SAP paragraphs 149-152 .* *149 A safety categorisation scheme could be determined on the following basis:* *a) Category A – any function that plays a principal role in ensuring nuclear safety.* *b) Category B – any function that makes a significant contribution to nuclear safety.* *c) Category C – any other safety function.* *150 The method for categorising safety functions should take into account:* *a) the consequence of failing to deliver the safety function;* *b) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;* *c) the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;* *d) the likelihood that the function will be called upon.* *151 The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components required to deliver the safety function.* *152 The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.*	The Compliance document refers out to the requirements of 10CFR50 App A Criterion 2 and 10CFR50.55a. In addition. Reference is made to the safety classification requirements of ANSI and ANS standards. In SSER Section 3.2, direct comparisons of the different standard requirements are made. SSER section 3.2 states that "Structures, systems, and components in the AP1000 are classified according to nuclear safety classification, quality groups, seismic category, and codes and standards." SSER Section 3.2.2 states that "The assignment of safety-related classification and use of codes and standards conforms to the requirements of 10 CFR 50.55a for the development of a Quality Group classification and the use of codes and standards" With SSER section 3.2 there is a detailed explanation of the safety classification philosophy, and a series of tables which identify the categories that individual structures and components are in. It should be noted that there is a separate classification scheme for seismic withstand requirements. It is considered that the requirements of this principle have been met.
Safety classification of structures, systems and components *Principle ECS.2 - Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.*	The compliance document refers to the response given for ECS.1, similarly, the assessment response can be seen under ECS.1 It is considered that the requirements of this principle have been met.

Assessment Topic/SAP	Assessment
Guidance - SAP paragraphs 153-156 . *153 The method for classifying the safety significance of a structure, system or component should primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:* *a) the category of safety function(s) to be performed by the item (see Principle ECS.1);* *b) the consequences of failure to perform its function;* *c) the probability that the item will be called upon to perform a safety function;* *d) the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.* *154 A safety classification scheme could be determined on the following basis:* *a) Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.* *b) Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.* *c) Class 3 – any other structure, system or component.* *155 Appropriately designed interfaces should be provided between structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.* *156 Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.*	
Standards *Principle ECS.3 - Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.* *Guidance - SAP paragraphs 157-161* *157 The standards should reflect the functional reliability requirements of structures, systems*	Within the UK Compliance Document (Reference 5), Under ECS 3, the following statement is made. "The industry codes and standards that apply to the design and procurement of safety-related components are specified in the DCD." Further, under ECS.4 and ECS.5, the following statements are made "The AP1000 uses only components with codes and

Assessment Topic/SAP	Assessment
and components and be commensurate with their safety classification. 158 *Appropriate national or international codes and standards should be adopted for Classes 1 and 2 of structures, systems and components. For Class 3, appropriate non-nuclear-specific codes and standards may be applied.* 159 *Codes and standards should be preferably nuclear-specific codes or standards leading to a conservative design commensurate with the importance of the safety function(s) being performed. The codes and standards should be evaluated to determine their applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the safety function(s) being performed.* 160 *Where a structure, system or component is required to deliver multiple safety functions, and these can be demonstrated to be delivered independently of one another, codes and standards should be used appropriate to the category of the safety function. Where independence cannot be demonstrated, codes and standards should be appropriate to the class of the structure, system or component (ie in accordance with the highest category of safety function to be delivered). Whenever different codes and standards are used for different aspects of the same structure, system or component, the compatibility between these should be demonstrated.* 161 *The combining of different codes and standards for a single aspect of a structure, system or component should be avoided or justified when used. Compatibility between these codes and standards should be demonstrated.*	standards already in practice." "The AP1000 is designed to codes, standards, and regulations as required by the NRC and documented in the DCD" Reference is made to the following standards American Concrete Institute (ACI), Code Requirements for Nuclear Safety Related Structures, ACI-349-01 American Institute of Steel Construction (AISC), Specification for the Design, Fabrication and Erection of Steel Safety Related Structures for Nuclear Facilities, AISC-N690-1994. American Society of Civil Engineers, "Minimum Design Loads for Buildings and Other Structures," ASCE 7-98 ASCE Standard 4-98, "Seismic Analysis of Safety-Related Nuclear Structures and Commentary," American Society of Civil Engineers, September 1998 It is also noted that reference is made to a number of WCAP documents, which are Westinghouse Internal Standards, the provenance of which has not been considered in this assessment. It is also noted that some specific non-nuclear codes have been used such as FEMA 356 as background justification for analysis and design. In addition, some of the standards referred to may have been superseded, for example, SRP 3.7.2, Rev2 1989, is now at Rev 3 2007. IEE-487 -1987 has now been superseded by a 2004 version and importantly, ACI 349-01 has been overtaken by ACI349-06 and AISC-N690-1994 by a 2003 version. The implications of this will be considered in Step3. There are no recognised international standards for nuclear structures, the ACI/ AISC codes for concrete and steel structures are well recognised as appropriate for this type of structure. It is considered that the requirements of this principle have been met.
`	
Failure to safety *Principle EDR.1 - Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.*	The compliance document does not discuss this principle in any level of detail for structures, but refers out to the DCD sections where the design codes used are detailed. These, as expected are US codes of practice. However, beyond this there is no further comment. Section 3.1 of the DCD gives further overview of design criteria, and is essentially a review of how the 10CFR50 AppA criteria are met. It is considered that the requirements of this principle have been met.
Defence in depth	

Assessment Topic/SAP	Assessment
Redundancy, diversity and segregation *Principle EDR.2 - Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety* *Guidance - SAP paragraph 170* *170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.*	As for EDR1, heavy reliance is placed on the satisfaction of the 10CFR50 requirements to satisfy this requirement. There is nothing specific in the DCD section 3.1,3.2 etc which provides additional evidence on this. The expectation is that through the use of design codes, these requirements will be met. From an external hazards perspective, the use of 4 trains each housed in separate structures gives a high degree of confidence that this requirement can be met. However, a more thorough review will be required at step 3 It is considered that the requirements of this principle have been met.
Common cause failure *Principle EDR.3 - Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.* *Guidance - SAP paragraph 171 - 174* *171 CCF claims should be substantiated.* *172 In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by NII of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment.* *173 Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the dutyholder for better figures. Such a case would not then be ruled out of consideration.* *174 Where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.*	The compliance document states that the AP1000 design has addressed this issue through the use of PRA. A brief inspection of SSER section 19.29 (Common Cause Analysis) does not give any further insights. However, the PRA document section 29 gives a more detailed consideration of this issue. It is considered that the requirements of this principle have been met.
Single failure criterion *Principle EDR.4 - During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.*	The compliance document makes the following claim "The AP1000 design basis ensures that no single random failure will prevent a safety system from performing its safety function. The AP1000 PRA considers beyond design basis accident sequences in which a single failure

Assessment Topic/SAP	Assessment
Guidance - SAP paragraph 175 *175 Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Further discussion of the single failure criterion is given in IAEA Safety Standard NS-G-1.2.*[4]	may cause failure of a safety system." It is considered that the requirements of this principle have been met.
External and Internal Hazards	
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 *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.*	Section 3.1.1 of the DCD states under Compliance with Criterion 2 of 10CFR50 App A "The safety-related structures, systems, and components are designed to withstand the effects of natural phenomena without loss of the capability to perform their safety-related functions, or are designed such that their response or failure will be in a safe condition. Those structures, systems, and components vital to the shutdown capability of the reactor are designed to withstand the maximum probable natural phenomena at the intended site. Accident analyses consider conservative site conditions that envelope expected sites. Appropriate combinations of structural loadings from normal, accident, and natural phenomena are considered in the plant design. The design of the plant in relationship to those natural phenomena is addressed." Section 2.1 of the DCD gives an overview of the hazards inherent in the design of the plant, and also identifies those aspects which will require more detailed consideration at the site selection stage. Sections 3.3- 3.11 of the DCD provide further details of the hazard derivation. It is noted that there is no apparent mention of lightning as an external hazard. The process for identification and screening of all external hazards is not readily apparent from the documents reviewed, however it is recognised that those most likely to influence the design have been recognised. A more complete review of this will be required in Step3. It is considered that the requirements of this principle have been met.
Principle 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 214 Some hazards may not be amenable to the derivation of a design basis event. Such hazards may include fire and lightning, but are addressed through appropriate application of codes and standards	There is no attempt at this stage to relate the external hazards used in the design to a probabilistic level. However, there is equally no attempt to screen out hazards, and the documents provide confidence that a suitable range of hazards has been considered in the design, although Step3 will consider this in more detail. It is considered that the requirements of this principle have been met.
Principle EHA.4 - The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance of no more than once in 10 000 years 215 Consideration may also be given to arguments presented to derive the design basis event from a higher frequency of	The AP1000 design envelope has been derived primarily from US requirements, and this is not readily transferable to the UK situation. A brief examination of the major hazard magnitudes as detailed in DCD section 2.1 shows that the values used appear to be broadly compatible with those derived for existing UK sites. It is considered that the requirements of this principle have been met.

Assessment Topic/SAP	Assessment
exceedance if the facility cannot give rise to high, unmitigated doses. 216 Where the radiological consequences arising from an external hazard are low, it may be appropriate for a facility to be designed to hazard loads using normal industrial standards.	
Principle EHA.5 - Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition	The compliance document states that "DCD Section 3.1 reports on how the AP1000 responds to the General Design Criteria from 10 CFR 50, Appendix A. Criterion 2 from 10 CFR 50, Appendix A is the "Design Bases for Protection Against Natural Phenomena." Included in this criterion is the statement that the design bases shall reflect appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena. In response, the AP1000 design has accident analyses that consider conservative site conditions that envelope expected sites. Appropriate combinations of structural loadings from normal, accident, and natural phenomena are considered in the plant design." It is considered that the requirements of this principle have been met.
Principle EHA.6 - Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects 217 To achieve the above two 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 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 (eg 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.	The response toEHA.5 above covers this.

Assessment Topic/SAP	Assessment
Civil Engineering	
ECE.1 - The required safety functional performance of the civil engineering structures under normal operating and fault conditions should be specified	Section 3.2 of the DCD summarises the safety classification system used in the design process. Furthermore, there are tables identifying the design requirements for each of the key structures It is considered that the requirements of this principle have been met.
ECE.6 - For safety-related structures, load development and a schedule of load combinations within the design basis together with their frequency should be used as the basis for the design against operating, testing and fault conditions. 288 For more severe loadings of structures that provide a principle means of ensuring nuclear safety, predicted failure modes should be gradual, ductile and, for slowly developing loads, detectable. 289 The data from the devices and measurements referred to in paragraph 298 should be used during the periodic reviews of the safety case or in post-event analysis for civil structures.	Tables 3.8.4-1 and 3.8.4-2 identify the load combinations for the Category 1 Concrete and Steel structures It is considered that the requirements of this principle have been met.
ECE.12 -. Structural analysis or model testing should be carried out to support the design and should demonstrate that the structure can fulfil its safety functional requirements over the lifetime of the facility 292 The analysis or model testing should use methods and data that have been validated and verified.	Section 3.8 of the DCD provides the principles and standards to be used in the design and analysis of safety critical structures. There are definitions of and references out to appropriate quality standards that apply to this activity. It is considered that the requirements of this principle have been met.
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*	The Compliance document states that "The AP1000 has been designed such that safety systems have adequate separation, redundancy/diversity, and protection so that required safety functions cannot be disabled by internal or external hazards. Chapter 3 of the DCD, "Design of Structures, Components, Equipment, and Systems," specifies the AP1000 conformance with NRC General Design Criteria, wind and tornado loadings, flood design, missile protection, protection against the dynamic effects of pipe rupture, seismic design, and seismic and environmental qualification. Additionally, the AP1000 PRA includes the evaluation of risk at power operation, low power operation, and at shutdown from both internal and external events. DCD Section 19.59, provides a summary of these PRA results." It is considered that the requirements of this principle have been met.

Assessment Topic/SAP	Assessment
working of the safety system.	
Containment and Ventilation	
ECV.3 - The primary means of confining radioactive substance should be by the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components. 424 Where appropriate, containment design should: a) define the containment boundaries with means of isolating the boundary; b) establish a set of design safety limits for the containment systems and for individual structures and components within each system; c) define the requirements for the performance of the containment in the event of a severe accident as a result of internal or external hazards, including its structural integrity and stability; d) include provision for making the facility safe following any incident involving the release of radioactive substances within or from a containment, including equipment to allow decontamination and post-incident re-entry to be safely carried out; e) minimise the size and number of service penetrations in the containment boundary, which should be adequately sealed to reduce the possibility of nuclear matter escaping from containment via routes installed for other purposes; f) avoid the use of ducts that need to be sealed by isolating valves under accident conditions. Where isolating valves and devices are provided for the isolation of containment penetrations, their performance should be consistent with the required containment duties and should not prejudice adequate containment performance; g) provide discharge routes, including pressure relief systems, with treatment system(s) to minimise radioactive releases to acceptable levels. There should be appropriate treatment or containment of the fluid or the radioactive material contained within it, before or after its released from the system; h) allow the removal and reinstatement of shielding;	The UK compliance document states that "The AP1000 design includes a sealed containment structure with extremely low leakage. The AP1000 passive safety system design has greatly reduced the number of containment penetrations, the majority of which are isolated by air-operated, fail-closed valves, or pressure-actuated check valves, which require no active support systems." A greeter degree of scrutiny of this area will be undertaken as part of Step3. It is considered that the requirements of this principle have been met.

Assessment Topic/SAP	Assessment
i) define the performance requirements of containment systems to support maintenance activities; j) demonstrate that the loss of electrical supplies, air supplies and other services does not lead to a loss of containment nor the delivery of its safety function; k) demonstrate the control methods and timescales for re-establishing the containment conditions where access to the containment is temporarily open (eg during maintenance work); l) incorporate measures to minimise the likelihood of unplanned criticality wherever significant amount of fissile materials may be present. 425 Should the pressure relief system operate, the performance of the containment should not be degraded	

Annex 2

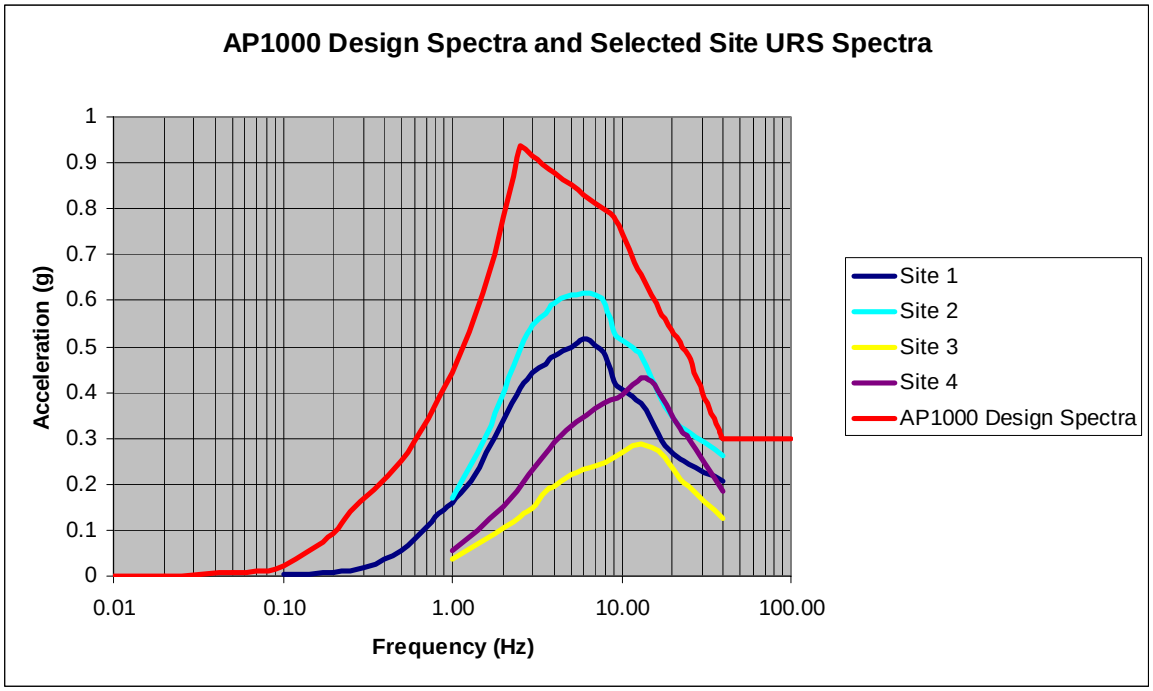
Generic Site Consideration

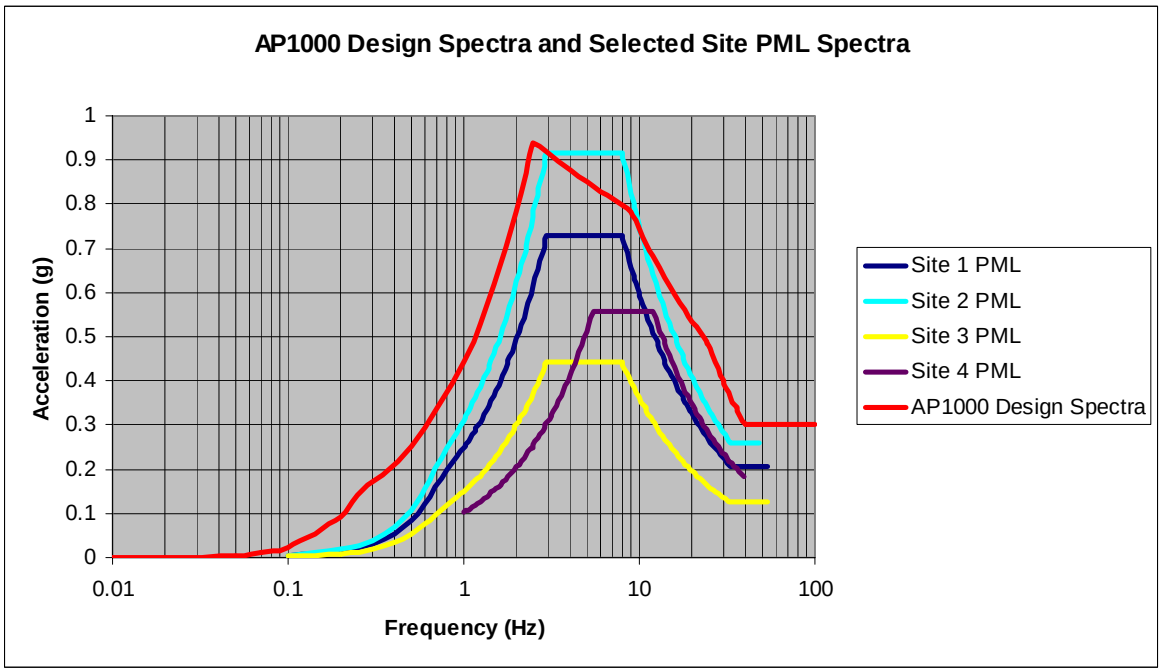
Requirement	Documentary Evidence	Judgement over acceptability
Site Characteristics assumed are detailed in a clear and unambiguous manner	Table 2-1 of DCD section 2.o provides a description of the site assumed in the design	At Step 2, this is adequate
Site Characteristics are related to design standards	The design standards used are all US in origin, as are the site characteristics, there is therefore a direct link	At Step 2, this is adequate
Design Standards are linked to UK specific application	None at this stage, however recognition that this will need to be done	At Step 2, this is adequate

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Seismotectonic				
Earthquakes	3.7	3.7	N	
Long period ground motion				X
Liquefaction	2.5.4	N	N	
Dynamic compaction	2.5.4	N	N	
Flooding				
Extreme Rainfall	**2.3**	**2.3**	**N**	
Tidal Effects	**3.4**	**N**	**N**	
Storm Surge	**3.4**	**N**	**N**	
Seiche	**3.4**	**N**	**N**	
Tsunami	**3.4**	**N**	**N**	
Dam Failure	**2.5**	**N**	**N**	
Watercourse containment failure	**3.4**	**N**	**N**	

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Meteorological				
Weather Effects	**2.3**	**2.3**	**N**	
High Wind	**2.3**	**2.3**	**N**	
Extreme Drought	**2.3**	**2.3**	**N**	
Extremes of Air Temperature	**2.3**	**2.3**	**N**	
Extremes of ground temperature	**2.3**	**2.3**	**N**	
Extremes of Sea (or river) Temperature				**X**
Lightning				**X**
Extreme Hail, Sleet or Snow and Icing	**2.3**	**2.3**	**N**	
Humidity				**X**
Climate Change (Affects many of the above)				**X**
Man Made				
Accidental Aircraft Impact	**3.5**	**N**		
Impacts from Adjacent sites	**2.2**	**N**		
Gas Clouds (toxic, asphyxiates, flammables)	**3.5**	**N**		
Liquid Releases (flammables, toxic, radioactive)	**3.5**	**N**		
Fires				
Explosions (blast waves, missiles)	**3.5**	**N**		
Missiles (turbines, bottles BLEVE)	**3.5**	**N**		
Transport (road, sea, rail)	**2.2**	**N**		
Electromagnetic Interference				**X**
Pipelines (Gas, Oil, Water)	**2.2**	**N**		
Vibrations	**2.2**	**N**		
Sabotage	**TQ00006**			

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Biological				
Biological Fouling				X
Seaweed				X
Fish				X
Jellyfish				X
Marine growth				X
Infestation				X
Geological				
Settlement	2.5	N	N	
Ground heave				X
Mining (inactive or active)				X
Caverns				X
Groundwater	2.5	N	N	
Leeching				X
Contaminated land				X
Landslides	2.5	N	N	
Radon				X
Fissures				X
Faults	2.5	N	N	





Notes

URS are Uniform Risk Spectra Developed for use in Periodic Safety Review Assessment of Existing Plant, Seismic Margins and PRA. The 10^{-4} pa probability of exceedance values are shown.

PML are Principia Mechanica Limited Spectra. These were developed for use as broad band spectra for use in design of UK critical facilities. They are developed from a knowledge of the anticipated pga at the site and the site ground conditions. Those shown have been anchored to the 10^{-4} pa probability of exceedance pga values.

Figure 1 Comparison of AP-1000 Design Spectra with various UK site Response Spectra