

**HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT**

New Build

STEP 2 AECL ACR-1000 Civil Engineering and External Hazard Assessment

Bootle
Merseyside L20 7HS

1. INTRODUCTION

This assessment report records the Step 2 Siting, Civil Engineering and External Hazards assessment of the Atomic Energy Canada Limited (AECL) Advanced Candu Reactor (ACR) 1000 submission in accordance with the strategy outlined in Ref 2.

Overall, it was concluded that the AECL claims against the key Siting, Civil Engineering and External Hazard Safety Assessment Principles (SAPs) used for Step 2, were reasonable. However, supporting arguments and evidence will be required, during Steps 3 & 4, to ensure that the ACR-1000 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 AECL 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 two.

This assessment report covers the Siting, External Hazard 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 AECL 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 AECL Step 2 submission used during the assessment was located at S:\New Reactor Build\RP Submissions\AECL Submission – Sept 2007.

A separate submission by AECL, Ref 5, presented a discussion on how the ACR-1000 design addressed a selection of the principles in the HSE Safety Assessment Principles for Nuclear Facilities, Ref 6, and included cross references to the SER.

AECL claim that the ACR-1000 has addressed all relevant UK Safety Assessment Principles (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

AECL claim that the ACR-1000 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 some other 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.

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 clearly a need to examine the impact on the population around a site. This has been addressed in a separate assessment report. AECL 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 AECL need to better understand the siting Policy for Nuclear Reactors in the UK.

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

AECL claim that the ACR-1000 design has addressed these SAPs, Ref 5. There is a safety classification system in place. When applied to structures, there is a lack of clarity over the link to design basis for the various structures other than for the containment. The design standards quoted are primarily CANDU specific or Canadian, however there is also considerable reference to American standards and NUREGs. The standards referred to appear, where necessary, to be specific to Nuclear-grade structures. 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-Canadian/US Specification materials for construction. 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.

It was unclear from the initial submission if the prestressing tendons in the containment structure were grouted in place or free. AECL have clarified that the tendons are free within the ducts and are greased to assist in maintaining integrity. This approach is in line with existing UK practice for pre-stressed containment structures.

Observation 3 The links from design classification to design standards will need further investigation to ensure that the intent is satisfied. Clarity over the design classification for structures will need to be provided.

Observation 4 The standards used need to be understood better, especially those which appear to be CANDU / Canada specific.

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

There is little in the documents, thus far, that indicates the nature of the design envelope for the ACR-1000 in terms of limiting site characteristics. The only clue to this is given in section 3.3.1 of 10820-01371-TED-001-H where it states that *“Both containment structure and internal structures are supported on a common base slab. They are designed to withstand a design basis earthquake (DBE) and the site environmental requirements. The building is seismically qualified for a DBE of 0.3 g peak ground acceleration at rock or firm strata level and a wide range of soil/rock foundation conditions.”* This is something that will require further investigation during Step 3 as part of UK contextualisation.

2.3.3 External Hazards

AECL claim that the ACR-1000 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. The current list of hazards recognises that some cannot be defined until a site (or sites) have been identified. 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, Figure 1 in this report shows a basic comparison of the seismic design basis for the ACR-1000 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.

Observation 6 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 7 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. AECL claim that the ACR-1000 has been designed such that the safety systems have adequate separation, redundancy, diversity and protection so 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 8 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

It is noted that there is a specific recognition of the need to consider aircraft impact from a non-accidental standpoint. The nature and extent of this is not described in any degree of detail in the submitted documents. AECL have responded to our Technical Query ACR1000-000004. The response has confirmed that aircraft impact of a non-accidental nature has been considered as part of the design basis for the ACR-1000. This will be examined in more detail in Step 3.

2.3.4 CDM Regulations

There is no specific mention of the Construction Design and Management (CDM) Regulations 2007, 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 9 There needs to be a recognition that the Construction Design and Management Regulations 2007 will apply to this project.

3. CONCLUSION

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

Overall, it was concluded that the claims made by AECL, 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 ACR-1000 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 AECL in support of the claims.

4. RECOMMENDATION

1. The observations identified throughout this assessment report will require a response from AECL 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 Siting, External hazards and Civil Engineering Assessment Strategy”, Assessment Report No. AR07007
4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.
5. AECL Document 10820-01321-ASD-008-H Rev 0. “Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles.
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	
<p>Safety categorisation</p> <p><i>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.</i></p> <p><i>Guidance - SAP paragraphs 149-152.</i></p> <p>149 <i>A safety categorisation scheme could be determined on the following basis:</i></p> <ul style="list-style-type: none"> a) <i>Category A – any function that plays a principal role in ensuring nuclear safety.</i> b) <i>Category B – any function that makes a significant contribution to nuclear safety.</i> c) <i>Category C – any other safety function.</i> <p>150 <i>The method for categorising safety functions should take into account:</i></p> <ul style="list-style-type: none"> a) <i>the consequence of failing to deliver the safety function;</i> b) <i>the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;</i> c) <i>the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;</i> d) <i>the likelihood that the function will be called upon.</i> <p>151 <i>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.</i></p> <p>152 <i>The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.</i></p>	<p>The compliance document states that</p> <p><i>“The SSCs important to safety (ITS) of the ACR-1000 are categorized based on their safety functions. Appropriate design requirements are then applied individually to the structures, systems, and components, based on the importance of the safety function. The requirements take into account the consequences of the potential failures and the failure frequency.”</i></p> <p>Reference is also made to document 108-03650-SDG-001-H“Safety Classification of Structures Systems and Components”. <i>“This document provides further details and also states that This classification is based on the requirement outlined in IAEA NS-R-1”</i></p> <p>Within the document, 108-03650-SDG-001-H the philosophy for safety categorisation of SSC’s is outlined in more detail. This is clear for the systems, however the categorisation for structures other than the containment is unclear from the document supplied. This will need to be investigated further in Step 3.</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Safety classification of structures, systems and components</p> <p><i>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</i></p>	<p>See response to ECS.1</p>

Assessment Topic/SAP	Assessment
<p>significance with regard to safety.</p> <p>Guidance - SAP paragraphs 153-156 .</p> <p>153 <i>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:</i></p> <ul style="list-style-type: none"> a) <i>the category of safety function(s) to be performed by the item (see Principle ECS.1);</i> b) <i>the consequences of failure to perform its function;</i> c) <i>the probability that the item will be called upon to perform a safety function;</i> d) <i>the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.</i> <p>154 <i>A safety classification scheme could be determined on the following basis:</i></p> <ul style="list-style-type: none"> a) <i>Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.</i> b) <i>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.</i> c) <i>Class 3 – any other structure, system or component.</i> <p>155 <i>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.</i></p> <p>156 <i>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.</i></p>	
<p>Standards</p> <p><i>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.</i></p> <p>Guidance - SAP paragraphs 157-161</p>	<p>The compliance document states that</p> <p><i>“The SSCs Important to Safety of the Advanced CANDU Reactor (ACR) are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected according to the AECL formal design documents manual (FDDM), new build CANDU quality assurance manual (QAM), plant performance specifications (PPS), safety design guides (SDGs), analysis basis reports (AB), analysis reports (AR), design control documents (DCD), design descriptions (DD), design guides (DG),</i></p>

Assessment Topic/SAP	Assessment
<p>157 <i>The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification.</i></p> <p>158 <i>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.</i></p> <p>159 <i>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.</i></p> <p>160 <i>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.</i></p> <p>161 <i>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.</i></p>	<p>design manuals (DM), design requirements (DR), and technical specifications (TS) and examination, maintenance, inspection and testing schedules (EMITS).””Those AECL documents refer to and comply with applicable Canadian nuclear standards set by the Canadian Standard Association (CSA) for the design, manufacturing, construction, installation, commissioning, quality assurance, maintenance, testing and inspection of the SSCs Important to Safety. In addition to the Canadian Standards Association (CSA) codes and standards, appropriate sections of other industrial standards, such as the Instrument Society of America (ISA) standards, Military Standards (MIL) and Institute of Electrical and Electronics Engineers (IEEE) standards are applied as appropriate to the design of systems, structures, and components. The ACR design will also comply, to the extent applicable, with the requirements outlined in relevant International guides, such as those of the International Atomic Energy Agency (IAEA)”</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Failure to safety</p>	
<p><i>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.</i></p>	<p>The compliance document states that</p> <p>“The ACR-1000 design and the processes used to perform the design development comply with this Principle. The proven CANDU features which are used in the ACR-1000 design help to avoid failure modes and minimise the consequences of failures” In addition, reference is made to fault tree analysis, FMEA and human error analysis, as well as the requirements of Canadian regulatory guidance on this issue.</p> <p>It is considered that the requirements of this principle have been met.</p>

Assessment Topic/SAP	Assessment
<p>Defence in depth</p>	
<p>Redundancy, diversity and segregation</p> <p><i>Principle EDR.2 - Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety</i></p> <p><i>Guidance - SAP paragraph 170</i></p> <p>170 <i>It should be demonstrated that the required level of reliability for their intended safety function has been achieved.</i></p>	<p>The compliance document states that</p> <p><i>"In CANDU design, a high standard of design and engineering practices have been adopted to prevent the failure of normally operating systems; components are built to accepted standards; high-quality materials are selected; and principles of redundancy, diversity, separation, and independence are applied. These principles of diversity, redundancy, and independence are thus applied to the ACR-1000 design."</i> In addition, reference is made to the physical separation guidelines provided in the design standards, the use of PSA in the design, and the detailed consideration of dependent failures undertaken as part of the design process.</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Common cause failure</p> <p><i>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.</i></p> <p><i>Guidance - SAP paragraph 171 - 174</i></p> <p>171 <i>CCF claims should be substantiated.</i></p> <p>172 <i>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 Nil 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.</i></p> <p>173 <i>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.</i></p> <p>174 <i>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.</i></p>	<p>The compliance document states that</p> <p><i>"The ACR-1000 is designed according to the safety design guide on 'Separation of Systems and Components' [16], which ensures that common cause failures are explicitly addressed, where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability".</i> There is some high level discussion on how this is applied into protections against external hazards, and into civil structures.</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Single failure criterion</p>	<p>The compliance document states that there are three key contributors to</p>

Assessment Topic/SAP	Assessment
<p><i>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.</i></p> <p><i>Guidance - SAP paragraph 175</i></p> <p>175 <i>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</i></p>	<p>this, that</p> <p>"a) Minimizing the probability of failure of the components of these systems by adopting quality standards commensurate with their importance to the safety;</p> <p>b) Designing these systems to withstand the loads and adverse environmental conditions induced by the design basis events (including seismic event, fire, internal flooding etc.) through qualification and/or protection;</p> <p>c) Designing these systems to be tolerant of failures without loss of their safety functions.</p> <p>With respect to Item c), the types of failures that must be taken into account in the design of systems important to safety required for the design basis events include random failures and common cause failures. The concept of a random failure is applied to active as well as to passive components, where credible "</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>External and Internal Hazards</p>	
<p><i>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</i></p> <p>211 <i>This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.</i></p> <p>212 <i>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.</i></p> <p>213 <i>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.</i></p>	<p>The compliance document states that "All internal hazards and a generic set of external hazards are identified as part of the design development and included in the design basis assessment and the PSA. External hazards relevant to a specific UK site will be determined and assessed where they are not bounded by the generic set" A review of 10820-03600-ASD-001-H "ACR events" confirms that a wide range of events have been considered. In addition, there are a series of identified coincident and secondary effects identified.</p> <p>It is considered that the requirements of this principle have been met.</p>
<p><i>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</i></p> <p>214 <i>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</i></p>	<p>The compliance document notes that when a suitable site is identified, appropriate data will be used to establish the site hazard. The site characteristic upon which the design has been based is detailed in the "Site Characteristics document". There is recognition that some data cannot be established with any degree of certainty until a site or sites have been defined.</p> <p>It is considered that the requirements of this principle have been met.</p>

Assessment Topic/SAP	Assessment
<p>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</p> <p>215 Consideration may also be given to arguments presented to derive the design basis event from a higher frequency of exceedance if the facility cannot give rise to high, unmitigated doses.</p> <p>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.</p>	<p>The compliance document states that a wide set of Canadian based hazards have been use in the design, and that site specific values for the UK will be used to determine individual site demands.</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Principle EHA.5 - Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition</p>	<p>The compliance document states that "Compliance is ensured by the existing CANDU practice which assumes that the plant is being operated at the outer envelope of permitted operating states and with the minimum allowable plant availability."</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>Principle EHA.6 - Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects</p> <p>217 To achieve the above two principles the analysis should take into account that:</p> <ul style="list-style-type: none"> 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. 	<p>The compliance document states that</p> <p>"Compliance is ensured by the existing CANDU practice, updated to satisfy the intent of CNSC Regulatory Standards S-310 and IAEA NS-G-1.2 for safety analyses that will take into account simultaneous effects, common cause failure, defence in depth and consequential effects."</p> <p>It is considered that the requirements of this principle have been met.</p>

Assessment Topic/SAP	Assessment
Civil Engineering	
<p>ECE.1 - The required safety functional performance of the civil engineering structures under normal operating and fault conditions should be specified</p>	<p>The compliance document states that</p> <p>"All civil engineering structures are categorised and identified. The objective is to determine whether they are important to safety or not. Civil structures are categorised according to the potential consequences of their failure and their safety functions are explicitly stated in the plant Safety Design Guides. The required performance of the structures under all normal operating and fault conditions are specified and detailed as part of the Design Requirements and the Design Criteria for each structure."</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>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.</p> <p>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.</p> <p>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.</p>	<p>The compliance document states that</p> <p>"It is the CANDU practice that the load development and a schedule of load combinations within the design basis together with their frequency are used as the basis for the design against operating, testing and fault conditions for structures important to safety."</p> <p>It is considered that the requirements of this principle have been met.</p>
<p>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</p> <p>292 The analysis or model testing should use methods and data that have been validated and verified.</p>	<p>The compliance document states that</p> <p>"Methodologies of structural analyses or model testing/data used in the ACR-1000 design are well recognized by the industry and they have been validated and verified."</p> <p>It is considered that the requirements of this principle have been met.</p>
Safety Systems	
<p>Failure independence</p> <p><i>Principle ESS.18 - No fault, internal or external hazard should disable a safety system.</i></p> <p><i>Guidance - SAP paragraph 352</i></p> <p>352 <i>Safety systems should be physically separate, independent, isolated from other systems,</i></p>	<p>The compliance document states that</p> <p>"The ACR-1000 design complies fully with this principle. The safety systems in the ACR-1000 design are fully capable of mitigating all design basis events with due account taken of common cause failures."</p>

Assessment Topic/SAP	Assessment
<p><i>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.</i></p>	<p>It is considered that the requirements of this principle have been met.</p>
<p>Containment and Ventilation</p>	
<p>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.</p> <p>424 Where appropriate, containment design should:</p> <ul style="list-style-type: none"> 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 	<p>The compliance document states that</p> <p>The basic function of the containment system is to form a continuous, pressure-retaining envelope around the reactor core and the heat transport system. This limits releases to the external environment of radioactive material resulting from an accident. An accident that causes a release of radioactive material to containment may or may not be accompanied by a rise in containment pressure. The containment system includes the steel-lined, prestressed concrete reactor building containment structure, access airlocks, containment cooling spray for pressure reduction, and a containment isolation system, consisting of valves in certain process lines and ventilation ducts that penetrate the containment structure. This containment design ensures a low leakage rate and, at the same time, ensures integrity of the pressure-retaining boundary for all design basis events.</p> <p>Penetrations through the containment envelope will be designed with isolation devices as appropriate, to enable secure closure necessary to meet the minimum performance requirements for the containment, as required by SDG-006. The isolation devices will have sufficient redundancy, reliability and performance capabilities that reflect the importance to safety of isolating the penetration. The design of the isolating devices and penetrations will satisfy the reference dose limits for design basis accidents that release radioactivity into containment. The penetrations, including the isolation devices, will be considered part of the containment envelope. The isolating devices for penetrations that are open during normal plant operation will be testable. SDG-006 "Containment" lists the penetration requirements as follows:</p> <ul style="list-style-type: none"> a) The number of penetrations through the containment shall be kept to a practical minimum. b) All penetrations through the containment shall meet the same design requirements as the containment structure itself. They shall be protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles, jet forces and pipe whip. c) If resilient seals (such as electrometric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have the capability for leak testing at the containment design pressure, independent of the determination of the leak rate of the containment as a whole, to demonstrate their continued integrity over the lifetime of the plant. <p>Adequate consideration shall be given to the capability of penetrations to</p>

Assessment Topic/SAP	Assessment
<p>should be appropriate treatment or containment of the fluid or the radioactive material contained within it, before or after its released from the system;</p> <ul style="list-style-type: none"> h) allow the removal and reinstatement of shielding; 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. <p>425 Should the pressure relief system operate, the performance of the containment should not be degraded</p>	<p>remain functional in the event of a severe accident.</p> <p>It is considered that the requirements of this principle have been met.</p>

Annex 2
Generic Site Consideration

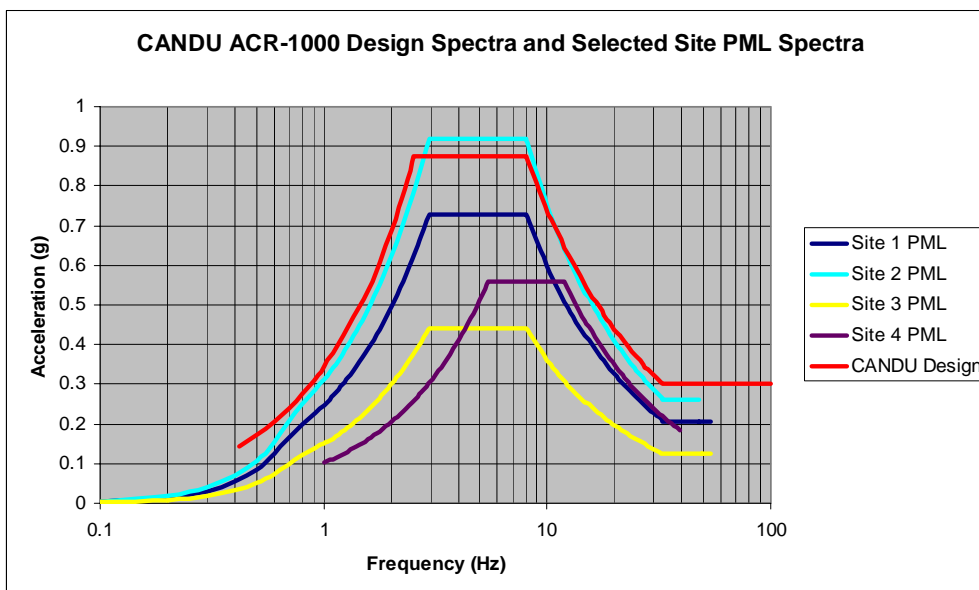
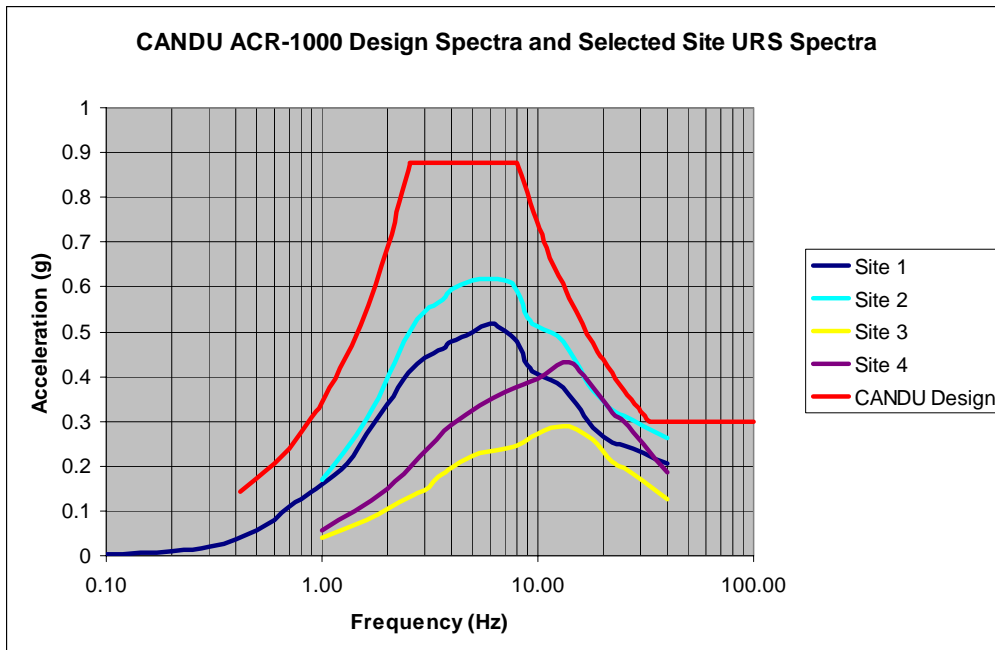
Requirement	Documentary Evidence	Judgement over acceptability
Site Characteristics assumed are detailed in a clear and unambiguous manner	Document 108-10100-PPS-001-H. "Site Characteristics PPS" provides details of the site characteristics see Table 2-1	At Step 2, this is adequate
Site Characteristics are related to design standards	The design standards used are all US / Canadian 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
<u>Seismotectonic</u>				
Earthquakes	2.5.2	N	N	
Long period ground motion				X
Liquefaction	2.5.4	N	N	
Dynamic compaction	2.5.4	N	N	
<u>Flooding</u>				
Extreme Rainfall	2.3.4	N	N	
Tidal Effects				X
Storm Surge				X
Seiche				X
Tsunami				X
Dam Failure				X

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Watercourse containment failure				
<u>Meteorological</u>				
Weather Effects	2.3	2.3	N	
High Wind	2.3.1,2.3.3	N	N	
Extreme Drought	2.4	N	N	
Extremes of Air Temperature	2.3	Tab 2-1	N	
Extremes of Ground Temperature	2.3	N	N	
Extremes of Sea (or river) Temperature				X
Lightning				X
Extreme Hail, Sleet or Snow and Icing	2.3	Tab 2-1	N	
Humidity	2.3	Tab 2-1	N	
Climate Change (Affects many of the above)				X
<u>Man Made</u>				
Accidental Aircraft Impact	2.2	N	N	
Impacts from Adjacent sites	2.2	N	N	
Gas Clouds (toxic, asphyxiates, flammables)	2.2	N	N	
Liquid Releases (flammables, toxic, radioactive)	2.2	N	N	
Fires				
Explosions (blast waves, missiles)	2.2	N	N	
Missiles (turbines, bottles BLEVE)	2.2	N	N	
Transport (road, sea, rail)	2.2	N	N	
Electromagnetic Interference	2.2	N	N	
Pipelines (Gas, Oil, Water)	2.2	N	N	
Vibrations	2.2	N	N	
Sabotage				

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
--------	---------------------	--------------------------	-------------	------------------------

<u>Biological</u>				
Biological Fouling				X
Seaweed				X
Fish				X
Jellyfish				X
Marine growth				X
Infestation				X
<u>Geological</u>				
Settlement	2.0	Table 2-1	N	
Ground heave				X
Mining (inactive or active)				X
Caverns				X
Groundwater	2.4	Table 2-1	N	
Leeching				X
Contaminated land				X
Landslides	2.5.4	N	N	
Radon				X
Fissures				X
Faults	2.5.3	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 ACR-1000 Design Spectra with various UK site Response Spectra