HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

Step 2 EPR 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 Electricite De France (EDF) and Areva United Kingdom European Pressurised Reactor (UK-EPR) submission in accordance with the strategy outlined in Ref 2.

Overall, it was concluded that the EDF/Areva 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 UK-EPR 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 EDF/Areva 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, Civil Engineering and External Hazards 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 EDF/Areva's claims 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 EDF/Areva Step 2 submission used during the assessment was located at S:\New Reactor Build\RP Submissions\EDF_AREVA Submission 1 - Aug 2007.

A separate submission by EDF/Areva, Ref 5, presented a discussion on how the UK-EPR design addressed a selection of the principles in the HSE Safety Assessment Principles (SAPs) for Nuclear Facilities, Ref 6, and included cross references to other documents.

EDF/Areva claims that the UK-EPR has addressed all relevant UK Safety Assessment Principles 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

EDF/Areva claims that the UK-EPR design has addressed these SAPs, Ref 5. The compliance document signposts to external hazards, which 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.

The aspect of population demographics around the installation has been recognised within the submission, and there is a clear understanding of the current UK planning policy. 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. As part of the ongoing Strategic Siting Assessment being undertaken by BERR, this issue is being considered further. EDF/Areva have recognised their position, and consider that the UK-EPR is equivalent to an AGR style design in terms of its position within the current Hansard Requirements.

Observation 1 *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

Reference 5 does not at present include any comments on the Civil Engineering SAPs. A review of the documentation supplied has shown that there is a safety classification system in place for structures, in terms of functional and performance requirements. This system is complex in nature, and whilst appearing to be logical and well structured will require further detailed scrutiny as part of Step 3.

The design standards quoted are EPR specific, namely the ETC-C code. A list of contents is provided within the Volume 2 submission, which indicates that all civil structures are designed according to this code. It is stated that the code has been developed using similar principles to the Eurocodes. Within Eurocode 1, however it is recognised that the eurocodes "*does not completely cover the design of special structures which require unusual reliability considerations*" and cites Nuclear Structures as an example. There is also passing reference to the ASME code for containment, and it is claimed there is equivalence with the ETC-C. The ETC-C code will require greater review at a principles level during Step 3 in terms of its development, benchmarking, accuracy and applicability.

One aspect, which does not appear to have been recognised, is the use of non-French 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.

The presented design for the inner concrete containment is a post-tensioned prestressed concrete structure, with the tendon ducts fully grouted. Within the UK, all the current PCPV's and the Sizewell B containment are prestressed concrete, however, the tendons remain free within the duct. This allows periodic inspection of both the load and condition of the tendons. This position is not mandated, however detailed consideration of the ability to maintain required prestress, and assurance over its level over the design life would be required, along with assurance over the long term condition of the tendons.

Observation 2 *The grouted duct design for the containment building is not an approach which has been accepted in the UK. Removal of tendons to allow routine inspection, and tightness checks is something which has become standard practice in the UK*

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 EPR specific. This primarily relates to ETC-C. It is noted that reference is made to principles in Eurocodes. Noting that Eurocodes are specifically ruled out as non-nuclear codes.*

Observation 5 *There needs to be recognition that non-French specification materials will be used for construction*

2.3.3 External Hazards

EDF/Areva claims that the UK-EPR 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. 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 UK-EPR 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*

Observation 7 *The process of load schedule development will require greater scrutiny in Step 3*

One of the requirements in SAP ESS.18 is to ensure that no external hazard should disable a safety system. EDF/Areva claim that the UK-EPR 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 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. Volume 2 Sub Chapter C.3, claims that the design has been modified since the events of 9/11 and that the design "takes into consideration all of the direct, indirect and potential consequences" of a commercial airliner impacting the Nuclear Island. This aspect will be reviewed in more detail in Step 3, against the requirements of the UK specific Design Basis Threat.

2.3.4 CDM Regulations

There is no specific mention of the Construction Design and Management Regulations 2007 (CDM) regulations that has been located in any of the submissions reviewed to date. This is unsurprising, as they have been primarily designed for submission to non UK areas, which do 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

EDF/Areva claims compliance with the key Siting, External Hazards and Civil Engineering SAPs in Appendix 1.

Overall, it was concluded that the claims made by EDF/Areva, 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 UK-EPR 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 EDF/Areva in support of the claims.

4. RECOMMENDATION

1. The observations identified throughout this assessment report will require a response from EDF/Areva 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. EDF AREVA Response to TQ EPR000003 “Compliance with HSE Safety Assessment Principles for Nuclear Installations (2006 Edition)”
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 states that EPR compliance with ECS.1 and ECS.2 is confirmed in SSER 1.E.5.3, (especially paragraph 5.3.1). The detailed implementation of those principles is reported in SSER 2.C.2. Implementation of safety classification in EPR is somewhat more complex than envisaged in the SAP. In particular: • Fundamentally, EPR uses two main classification systems: the first is termed “mechanical” and addresses pressure issues and barrier role of mechanical components (static approach); the second one is termed “functional” and addresses the performance of systems required by the accidents’ analyses (dynamic approach). • Both mechanical and functional classifications have evolved from the initial approach used on early PWR designs. The barrier approach, unchanged for the primary circuit, has been extended to cover the concept of activity retention whose consistency is ensured through the definition of two levels of risk. The functional classification has been adapted to address long term extension of the accidents’ analyses. Classification F1A is applied to the main safety systems (subject to single failure design criterion at the system level). Classification F1B is applied to systems required for longer term operation of the plant towards sustainable safe shutdown: it applies the concept of functional redundancy corresponding to IAEA meaning of the single failure principle. • Note that there is not an automatic correspondence between mechanical and functional classification levels. Even though a “typical” safeguard system is likely to be F1A / M2, other combinations are possible: e.g. F1A / M1 for primary circuit isolation, or F1A / M3 for most of the emergency feedwater system. On the other hand a few cross-requirements are postulated, e.g. no les than M3 for a mechanical equipment performing a F1 function, no less than F2 for the isolation between two different levels of mechanical classification (see SSER 2.C.2.1.10, in connection with paragraph 155 of ECS.2). • Mechanical and functional classifications give a comprehensive definition of component significance with regard to safety. Other so-called “classifications” describe

Assessment Topic/SAP	Assessment
	how this significance is interpreted in terms of relevant requirements in a specific technical field: C for buildings, E for I&C, EE for electrical equipments and SC for seismic 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.* *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.*	See Response to ECS1

Assessment Topic/SAP	Assessment
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 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.*	The compliance document states that EPR design is considered to comply with the SAP The objective of EPR safety classification is precisely to achieve through design, manufacturing and operating requirements, an acceptable quality of systems, components and civil structures involved in the plant safety. The safety classified systems, components and structures are arranged in classes, with corresponding requirements dependent on the safety functions to be performed. The most stringent requirements correspond to the most important safety functions. The following requirements may apply dependent on safety classification (see SSER 2.C.2): • for systems • single failure criterion • physical separation • emergency power supply • periodic tests for components • qualification • use of design and construction codes for both systems and components • design against earthquake • quality assurance During the plant life, the classified systems, structures and components will be inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance It is noted that the standards for design of the containment is as follows. The ETC-C (EPR Technical Code for Civil Works) is the code which serves as the basis for the design and construction of safety-classified civil works structures in the EPR. The current version of the ETC-C consist of three sections addressing the design requirements for the double-walled containment with a metal liner, procedures for construction and procedures for testing Reference is made to equivalence for containment structures to the requirements of the ASME RCC-M and RCC-MR codes. It is considered that the requirements of this principle have been met

Assessment Topic/SAP	Assessment
`	
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 states that The structures, systems and components (SSCs) important to safety are designed according to the general design requirements indicated in SSER 2.E. Safety classification of the SSCs is carried out using complementary approaches, and is extensively described in SSER 1.H: it results in stringent requirements expressed in terms of design and reliability. Moreover, redundant trains of the main safety systems (one per Safeguard Building) are strictly separated into four divisions. This operational separation is provided for electrical and mechanical safety systems. The four divisions of safety systems are consistent with the N+2 safety concept. With four divisions, one division can be out-of-service for maintenance and one division can fail to operate, while the remaining two divisions are available to perform the necessary safety functions even if one is ineffective due to the initiating event. This approach is complemented by PSA analyses where potential failure mode of systems and equipments were extensively evaluated The response does not specifically address the SAP towards buildings. A review of the codes used has shown that the ETC-C code has been used for the design basis. It is unknown to what degree this code incorporates the requirements above, however given its long use in France, it is considered unlikely that it would not. It is considered that the requirements of this principle have been met
Defence in depth	
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.*	The compliance document focuses on the requirements for systems rather than for structures as a whole. A review of Volume 2, section C5 provides confidence that a considered view over the levels of reliability/ performance under all load conditions has been undertaken. The details of the ETC-C code require further consideration as part of step 3 however. 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*	The compliance document states that Common cause failure is addressed for structures, systems and

Assessment Topic/SAP	Assessment
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.*	components important to safety. Reduced sensitivity to failures, including human errors, is achieved by: • adequate design margins, automation, high reliability of the devices in their expected environment and in the organisation of the operating team, protection against common mode failures by design against load cases (e.g. earthquake) This claim will require further investigation in Step 3 where the methods of qualification will be scrutinised in more detail. 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.* *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]	The compliance document state that "The design of structures, systems and components important to safety takes into account the single failure in order to ensure that more than the minimum number of components is provided to carry out any essential function. This requirement for redundancy assists in ensuring high reliability of safety classified systems designed to maintain the plant within its deterministic design basis" This claim will be reviewed further in Step3, especially in the context of External Hazards. 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	The compliance document states that

Assessment Topic/SAP	Assessment
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.*	EPR design is considered to comply with the SAP EPR is protected against the following external hazards (see SSER 1.E.5.5, 1.F.5.4 and 2.C.3): • Earthquake, • Aircraft crash, • External explosion, • Lightning and electromagnetic disturbances, • Groundwater, • Extreme meteorological conditions (high and low temperatures, snow, wind, rain, etc.), • External flooding, • Drought, • Ice formation, • Toxic, corrosive or flammable gas. Protection against the external hazards is achieved by designing the F1 classified safety equipment to withstand the loads associated with the hazard event, or by providing physical separation between redundant elements of a safety classified system so that their safety function can be performed despite the occurrence of the hazard. This design objective is to ensure that protection is provided against PCC design basis events despite the simultaneous occurrence of the external hazard. A review of the hazards identified indicates that a wide range has been considered at the design stage. A more complete review of the list along with scrutiny of any pre-design screening will be undertaken 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	The compliance document notes that when a suitable site is identified, appropriate data will be used to establish the site hazard. The site characteristics upon which the design has been based are 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. 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 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	There is no attempt found in the documentation to link the levels of hazard designed for against a frequency of exceedance.

Assessment Topic/SAP	Assessment
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 "Protection against the external hazards is achieved by designing the F1 classified safety equipment to withstand the loads associated with the hazard event, or by providing physical separation between redundant elements of a safety classified system so that the safety function can be performed despite the occurrence of the hazard. The design objective is to ensure that protection is provided against PCC design basis events despite the simultaneous occurrence of the external hazard. In designing the F1 classified structures, systems and components the hazard loading is combined with the most adverse plant operating conditions addressed in the design" This will require further scrutiny during Step 3 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 compliance document states that "Combinations of internal and external hazards are addressed in the EPR design (see SSER 2.C.3.1.3). Hazard loadings are combined when a link exists between the hazard conditions (e.g. flooding with extreme rainfall), where a hazard may arise as a consequence of another hazard (e.g. fire induced by aircraft crash) or where combining conditions from unrelated hazards is considered prudent for introducing conservatism into the design assessment, e.g. fire, postulated to occur after a controlled state has been reached following a PCC event or two weeks after a design basis earthquake or an RRC event. Safety classified systems and equipment required to bring the reactor to a final safety state in PCC design basis events are protected against internal and external hazards, either by being designed to withstand the hazard loads or by physical segregation of redundant trains of a safety system. In addition, the possibility of common cause failure of safety systems due to the hazard is addressed in the reactor design against RRC design extension conditions which consider total losses of redundant equipment. " This will require further scrutiny during Step 3 It is considered that the requirements of this principle have been met

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	The compliance document does not address this specifically. A review of Volume 2 Subchapter C5 has given confidence that there is a process in place for the identification of and the functional requirements under both normal and fault conditions, and that this is transmitted through to the design envelope definition. 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.	The compliance document does not address this specifically, however a review of the Volume 2, Chapter C.5 Table 1 and 2 provide evidence that this approach has been followed. The logic adopted has not been reviewed in detail, as this is a task for Step 3. 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.	The compliance document has not addressed this specifically. The design of the Civil Structures has been to an EDF document ETC-C. It is claimed that this is based on the principles laid down in Eurocodes. 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*	The compliance document states that "The EPR safety systems (extensively described in SSER 2.F) are physically separate, independent and isolated from other systems. SSER 2.C.3 and 4 explain how safety systems are protected against external and internal hazards. In addition, safety studies demonstrate that in case of one protection system failure, safety function can be ensured with other safety systems allowing the reactor to reach a safe state". It is considered that the requirements of this principle have been met

Assessment Topic/SAP	Assessment
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.	
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	The primary containment is the pressure vessel, and secondary containment via a double skin prestressed/ reinforced concrete structure The majority of plant required for normal operation is confined within the containment, with the primary penetrations being for steam supply, and safety trains. It is considered that the requirements of this principle have been met

Assessment Topic/SAP	Assessment
system; 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. 425 Should the pressure relief system operate, the performance of the containment should not be degraded	

Annex 2

Generic Site Consideration

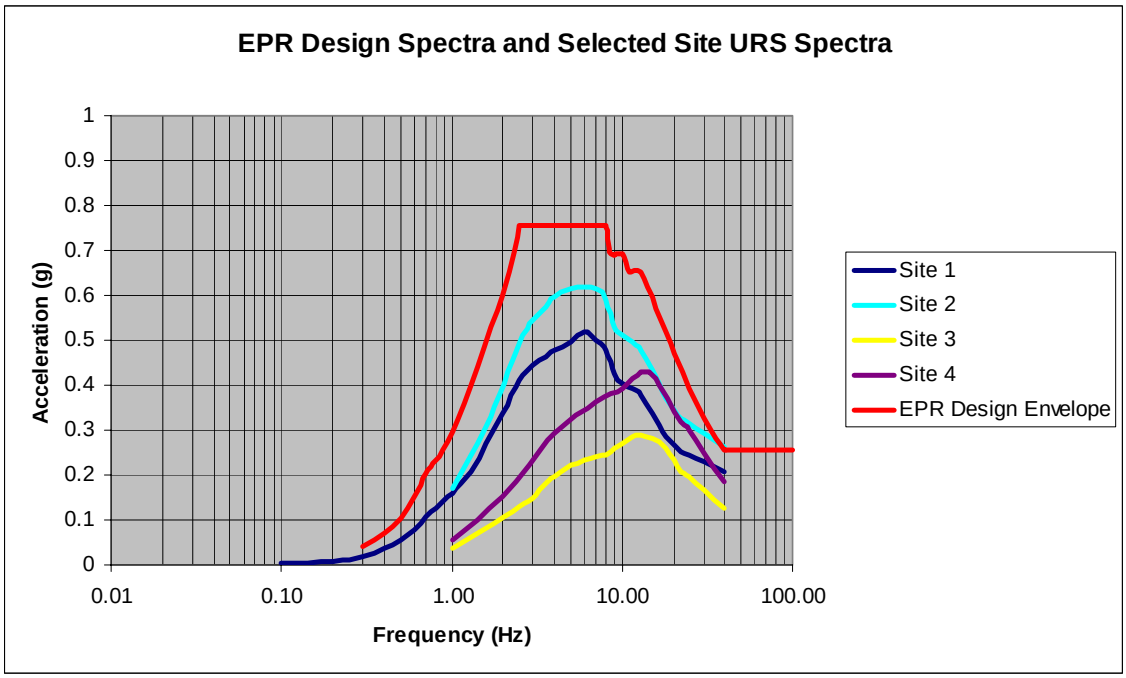
Requirement	**Documentary Evidence**	**Judgement over acceptability**
Site Characteristics assumed are detailed in a clear and unambiguous manner	Volume 1 Chapter D of the Head Document details the Generic Siting Envelope	At Step 2, this is adequate
Site Characteristics are related to design standards	The design standards used are based on those for the EPR in Flamanville and on the European Utility Requirements (EUR) for LWR power plants.	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

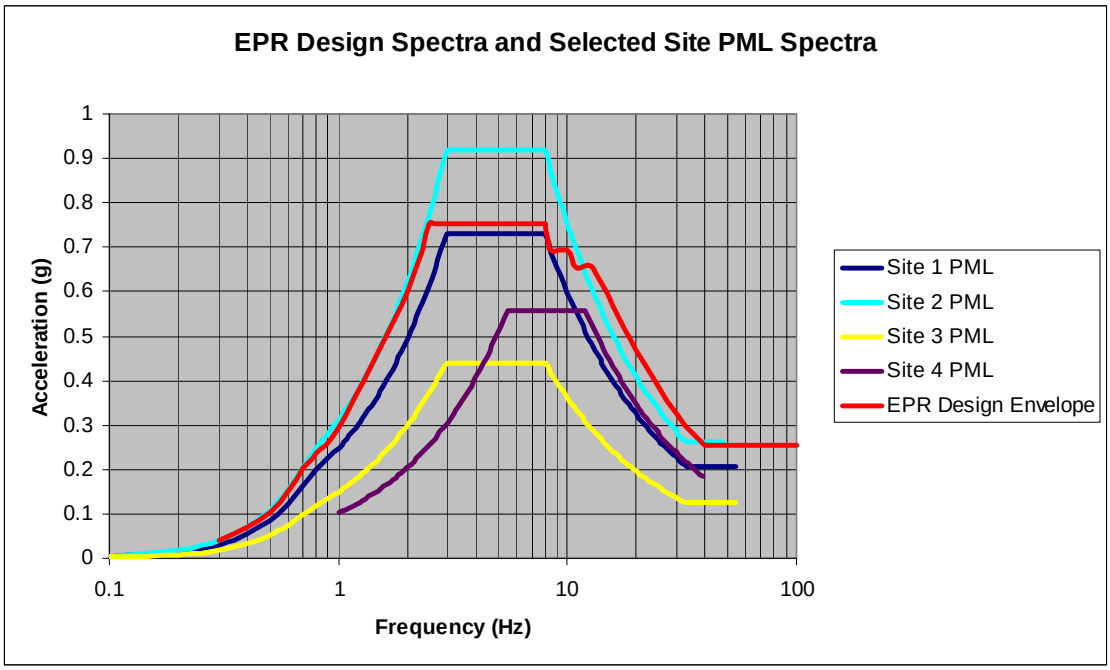
Hazard	**High Level Overview**	**Detailed Specific Demand**	**UK Specific**	**No Coverage Identified**
Seismotectonic				
Earthquakes	**V1 ChD 6.2**	**V2 ChC.3 Sec2**	**N**	
Long period ground motion				X
Liquefaction	**V1 ChD 6.2.2**	**V2 ChC.3 Sec2**	**N**	
Dynamic compaction				X
Flooding				
Extreme Rainfall	**V1 ChD 6.3.3**	**V2 ChC.3 Sec4**	**N**	
Tidal Effects	**V1 ChD 6.3.4**	**V2 ChC.3 Sec4**	**N**	
Storm Surge	**V1 ChD 6.3.5**	**V2 ChC.3 Sec V2 ChC.3 Sec44**	**N**	

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Seiche	**V1 ChD 6.3.6**	**V2 ChC.3 Sec4**	**N**	
Tsunami	**V1 ChD 6.3.7**	**V2 ChC.3 Sec4**	**N**	
Dam Failure	**V1 ChD 6.3.8**	**V2 ChC.3 Sec4**	**N**	
Watercourse containment failure	**V1 ChD 6.3.9**	**V2 ChC.3 Sec4**	**N**	
Meteorological				
Weather Effects				
High Wind	**V1 ChD 6.4.1**	**V2 ChC.3 Sec6**	**N**	
Extreme Drought	**V1 ChD 6.4.2**	**V2 ChC.3 Sec6**	**N**	
Extremes of Air Temperature	**V1 ChD 6.4.3**	**V2 ChC.3 Sec6**	**N**	
Extremes of ground temperature	**V1 ChD 6.4.4**	**V2 ChC.3 Sec6**	**N**	
Extremes of Sea (or river) Temperature	**V1 ChD 6.4.5**	**V2 ChC.3 Sec6**	**N**	
Lightning	**V1 ChD 6.4.6**	**V2 ChC.3 Sec7**	**N**	
Extreme Hail, Sleet or Snow and Icing	**V1 ChD 6.4.7**	**V2 ChC.3 Sec6**	**N**	
Humidity	**V1 ChD 6.4.8**	**V2 ChC.3 Sec6**	**N**	
Climate Change (Affects many of the above)	**V1 ChD 6.4.1**	**V2 ChC.3 Sec6**	**N**	
Man Made				
Accidental Aircraft Impact	**V1 ChD 6.5.1**	**V2 ChC.3 Sec3**	**N**	
Impacts from Adjacent sites	**V1 ChD 6.5.2**	**V2 ChC.3 Sec4**	**N**	
Gas Clouds (toxic, asphyxiates,	**V1 ChD 6.5.2.3**	**V2 ChC.3**	**N**	

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
flammables)		**Sec4**		
Liquid Releases (flammables, toxic, radioactive)	**V1 ChD 6.5.2.3**	**V2 ChC.3 Sec4**	**N**	
Fires				
Explosions (blast waves, missiles)	**V1 ChD 6.5.2**	**V2 ChC.3 Sec4**	**N**	
Missiles (turbines, bottles BLEVE)	**V1 ChD 6.5.2**	**V2 ChC.3 Sec4**	**N**	
Transport (road, sea, rail)	**V1 ChD 6.5.2**	**V2 ChC.3 Sec4**	**N**	
Electromagnetic Interference	**V1 ChD 6.5.2.2**	**V2 ChC.3 Sec7**	**N**	
Pipelines (Gas, Oil, Water)	**V1 ChD 6.5.2**	**N**	**N**	
Vibrations				
Sabotage	**V1 ChD 5**	**V2 ChC.3 Sec3**	**N**	
Biological				
Biological Fouling-				**X**
Seaweed				**X**
Fish				**X**
Jellyfish				**X**
Marine growth				**X**
Infestation	**V1 ChD 6.6.2**	**N**	**N**	
Geological				
Settlement				**X**
Ground heave				**X**
Mining (inactive or active)				**X**
Caverns				**X**
Groundwater				**X**
Leeching				**X**
Contaminated land				**X**

Hazard	High Level Overview	Detailed Specific Demand	UK Specific	No Coverage Identified
Landslides				X
Radon				X
Fissures				X
Faults				X





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 EPR Design Spectra with various UK site Response Spectra