Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 ELECTRICAL SYSTEMS ASSESSMENT OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/019-P

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

EXECUTIVE SUMMARY

My report presents the findings of the electrical engineering assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of GDA Step 3 of the HSE Generic Design Assessment (GDA) process. It provides an overview of the safety case presented in the PCSR, the standards and criteria adopted in my assessment and my preliminary assessment of the claims, arguments and evidence provided within the safety case.

For Step 3 of GDA, HSE's guidance requires the Requesting Party (RP) to provide a PCSR plus topic specific aspects. This guidance states that HSE will undertake an assessment, on a sampling basis, primarily directed at the system level and by analysis of the RP's supporting arguments. On the topic of electrical engineering this includes consideration of the following:

- Undertaking an initial assessment of the scope and extent of arguments in each of the technical areas, including the generic site envelope.
- Deciding on scope and plan of further assessment.
- Identifying requirements for additional regulatory verification/analysis.
- Judging whether the overall design is balanced in terms of the different contributors to overall risk from the plant

Westinghouse's safety claims and arguments are set out in the PCSR. These include the following claims and arguments:

- The main AC system does not perform any safety function.
- The battery backed Class 1E direct current (DC) and Uninterruptible Power Supply (UPS) systems provide reliable power for the safety systems, structures and components needed for shutdown of the plant.
- The standby diesel generators are not safety related as they do not support safety critical plant.

My assessment in the electrical engineering area only commenced part-way through GDA Step 3 so it has had to be limited in extent, concentrating on the overall electrical system integrity aspects. During GDA Step 4 I intend to make up the shortfall in GDA Step 3 coverage by intensifying the work of my Technical Support Contractor so that my assessment fully covers all of the work necessary to make the final judgement on the acceptability of the Electrical System as a part of HSE's Design Acceptance Conformation Process.

Westinghouse has confirmed in response to RO-AP-1000-042 (Ref. 11) that the following issues will be addressed for the Step 4 assessment:

- Safety functional categorisation and equipment classification of the AC power system. (Our preliminary view is that these should meet Class 2 Standards for safety systems.)
- Assessment of Codes and Standards applicable to UK design.
- Provision of higher tier electrical system report which demonstrates the adequacy of the Westinghouse design to meet safety requirements.

I conclude that the RP has provided a safety analysis that is generally satisfactory but there are still some areas where I believe that further work is required and that additional information needs to be provided. These are:

- Maintenance philosophy.
- DC system design, operation and monitoring.
- Electrical system studies and load flows.
- Electrical protection and relay discrimination.

- Transient stability studies.
- Safety classification of the diesel backed AC system
- Definition of applicable IEC codes and standards.
- Software and hardware verification for programmable devices.

The above will be targeted as a part of my plan for the Step 4 assessment.

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
BMS	(Nuclear Directorate) Business Management System
DCD	Design Control Document
EA	The Environment Agency
EMC	Electromagnetic Compatibility
EPRI	Electric Power Research Institute
FMEA	Failure Modes and Effects Analysis
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
NEMA	National Electrical Manufacturers Association
ND	The (HSE) Nuclear Directorate
US NRC	The United States Nuclear Regulatory Commission
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report
PRA	Probabilistic Risk Analysis
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
SAP	Safety Assessment Principle
SSC	System, Structure and Component
UL	Underwriters Laboratory
UPS	Uninterruptable Power Supply
WEC	Westinghouse Electric Company LLC
WENRA	The Western European Nuclear Regulators' Association

TABLE OF CONTENTS

1 INTRODUCTION

1 My report presents the findings of the Electrical Systems assessment of the Westinghouse AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the HSE Generic Design Assessment (GDA) process. My assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 2) and its associated guidance document G/AST/001 (Ref. 3). AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with the sampling of the safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 4) have been used as the basis for the assessment of the electrical systems associated with the AP1000 design. The SAPs require that electrical systems hazards on a nuclear power plant or nuclear chemical plant site be identified and considered in safety assessments. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 The role of the Step 3 assessment process is to identify any fundamental design aspects or safety shortfalls that could prevent the proposed design from being licensed in the UK. I have assessed the AP1000 electrical system using a subset of the Safety Assessment Principles (SAP) relevant to electrical power supply systems. My assessment was undertaken against each of these SAPs to confirm that an adequate claim of compliance exists within the Westinghouse submission. I have concluded that the claims are reasonable and the results of my assessment against the electrical SAPs are included in Annex 2 of this report. The arguments and evidence supporting these SAPs will be assessed during Step 4.

3 I have made a number of observations concerning the Westinghouse design and the Step 3 submission documentation. I have identified actions agreed with Westinghouse to address these observations to enable resolution for the Step 4 report.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

4 The main document setting out the Westinghouse safety case for electrical systems is the Design Control Document (DCD) (Ref. 5). The main claims detailed in this document are:

- The main AC system does not perform any safety related function.
- The battery backed Class 1E DC and UPS systems provide reliable power for the safety related equipment needed for shutdown of the plant.
- The standby diesel generators are not safety related as they do not support safety critical plant.

5 The passive design concept is based on AC power not being required to maintain the reactor in a safe state with all essential supplies being derived from battery systems. AC supplies from the main generator, grid and standby diesel generators are credited with providing defence in depth.

6 The safety demonstration classifies systems important to safety according to US custom and practice as determined by US NRC. This defines electrical systems in two classifications of safety-related and non-safety related.

7 The standards of design and construction for the electrical systems on the plant reference US standards IEEE, ANSI, NEMA, UL etc.

2.2 Standards and Criteria

8 The standards and criteria used for the electrical Step 3 assessment include:

- A subset of SAPs relevant to the electrical design.
- Relevant sections of HSE technical assessment guides and regulatory guidance.

2.3 Nuclear Directorate Assessment

2.3.1 Content of Requesting Party's Safety Case

9 The Westinghouse submission does not contain sufficient detail for a complete assessment of the scope and extent of the safety case. For the Step 4 submission more detail is required on the distribution network, safety categorisation, applicable standards and electrical protection and controls.

10 There is not sufficient information in the report to completely assess the design against all relevant SAPs. In particular, more information will be required on safety categorisation, maintenance and availability of safety systems, applicable standards and programmable devices (for example governors on diesel alternators and controls on static electrical conversion equipment).

11 More information is required in the Westinghouse submission to demonstrate that the detail design meets the safety objectives and that sufficient analysis and engineering substantiation has been performed to support an adequate demonstration that the plant will be safe.

12 The Westinghouse submission does not provide complete detailed descriptions of system architectures, their safety functions and reliability and availability requirements.

13 Confirmation and justification of design codes and standards is not provided in the Westinghouse submission. This can only be completed when the exercise to establish applicable design codes has been completed.

14 The safe operating envelope and operating regime have not been established in the Westinghouse submission as details are required on availability of systems to meet the claimed integrity.

15 The definition of which aspects of the design are complete has not been confirmed in the Westinghouse submission. This basis of the design for GDA purposes must be established to enable the assessment to be completed.

16 Westinghouse should ensure that the functional safety categorisation and system equipment safety classification is in line with international practice as defined in IEC 61226: 2009 (Ref. 7).

2.4 Comments on Requesting Party's Submission

17 There is insufficient detail in the Westinghouse submission to assess the validity of the arguments and evidence to support the safety claims made for the system. This will be required to be supplied by Westinghouse for assessment. The Westinghouse submission for Step 3 is defined in Chapter 8 of the Design Control Document. Requests for more detail on the design aspects have been met by the provision of further design documents in an unstructured manner. Westinghouse have committed in response to RO-AP1000-42 to provide a document entitled electrical system report which identifies the scope of the submission including all relevant documents.

18 The Westinghouse submission is based on meeting NRC requirements for safety which considers only two classes of safety related and non-safety related which does not align

with UK, IEC or IAEA practice. This approach results in claims that, for the passive system design of the AP1000, the only safety related systems are battery backed AC and DC systems. No formal safety claims are made for the AC diesel backed systems and no standards or availability requirements are specified. I conclude that this approach is unacceptable and that the diesel backed AC system should be Class 2 in accordance with UK, IEC and IAEA practice. In their response to RO-AP1000-42 (Ref. 11) Westinghouse has agreed to consider this classification and to modify the submission as appropriate. This will require the assessment to develop claims and arguments for the safety of the Class 2 AC system.

19 All existing Westinghouse documentation refers to US codes and standards in the form of references to IEEE, ANSI, NEMA, UL etc. In some instances these will be relevant where they refer to fundamental aspects of the reactor layout but where the documentation refers to standards for electrical equipment such as switchgear, transformers etc. then BS EN and IEC standards will apply. Westinghouse is addressing this issue by undertaking a fundamental review of codes and standards to prepare a comparison so that the submission can identify the codes and standards which will actually apply to a reactor built in the UK. Westinghouse response to RO-AP1000-42 (Ref. 11) confirms that the submission for Step 4 will include all the applicable codes and standards as a result of this review.

20 Clarification has been sought from Westinghouse on the use of software based programmable control devices on safety related systems. The requirements for the integrity of these devices were not initially addressed by Westinghouse but applying Class 2 to the diesel backed AC system requires the integrity to be addressed. It has been established that the principal application of programmable devices on the AC system is on electrical protection relays and on the main coolant pump frequency converters. For the Class 1E systems (mainly embedded controls on Static Conversion equipment and circuit breaker relays) the position is similar and therefore will need to be addressed. For the Step 4 assessment Westinghouse should provide detailed information on the use of programmable devices in all Class 1 and Class 2 equipment. It should also provide information on its approach to software safety justification for these devices.

21 There are two important claims made by Westinghouse associated with the grid connection and the main generator which contribute to the safety of the plant. The first is that the grid can remain stable and therefore feeding electrical energy to the station following a sudden loss of the main station generator. The second is that the main generator can continue to operate supplying the station house load in the event of a loss of grid connection fault. Westinghouse should supply more evidence on these transients during Step 4.

22 The standby diesel generators are located in a common building separated by three hour fire wall. For the Step 4 assessment Westinghouse are required to demonstrate that this arrangement can meet the safety claims for a Class 2 system particularly with regard to any single event which could cause the loss of both standby diesel generators.

23 The claims for the diesel generators for Step 4 need to take into account the potential for loss of both grid and diesel supplies from a division due to a fault on the main busbar of the diesel backed Class 2 switchboard. The claims for the availability of each diesel need to be determined in terms of allowable time out of service during reactor operation.

24 The results of system studies of the electrical system using a standard software package accepted by ND are required to be supplied by Westinghouse for the Step 4 submission. These will include demonstrations of load flows, fault studies and protection settings to achieve system co-ordination.

25 My assessment against SAP EQU.1 identified requirements for documentation of design verification requirements for electrical equipment preferably by type testing. A clear

statement of requirements for design verification is required which includes distinction between type testing and routine testing.

26 To complete my assessments against a number of the SAPS I require more information to be provided by Westinghouse. These requirements are defined against the relevant SAP.

27 Areas for further investigation have been identified against SAP EDR.3 which addresses common cause failure. Studies to address the potential for and effects of transient overvoltages and the effects of unearthed power systems should be carried out.

28 The assessment against SAP EMT.1 which covers maintenance inspection and testing identifies a requirement for a statement of maintenance philosophy including details of maintenance intervals and availability of electrical equipment

29 A further requirement identified against SAP EMT.1 is for the design of the battery monitoring system to be addressed to ensure that it is adequate to meet the system requirements.

3 CONCLUSIONS AND RECOMMENDATIONS

30 Westinghouse has provided adequate documentation for claims of compliance for the electrical system architecture defined against the electrical SAPs. In a number of areas I have identified that more detailed information should be provided in the Step 4 submission to so that I can complete my examination of the arguments and evidence in support of the claims.

31 A number of actions have been agreed with Westinghouse which will have to be satisfactorily resolved during the Step 4 process. Commitments have been made by Westinghouse to resolve these issues in the Step 4 submission. The issues which require to be addressed are:

- Safety Functional Categorisation and System Safety Classification of the AC system.
- Electrical Codes and Standards assessment.
- Software verification for programmable electrical protection relays and other embedded controls for Class 1 and 2 systems.
- Confirmation of design basis with single line drawings and applicable design documents.
- Preparation of complete claims, arguments and evidence to support the submission.

32 My assessment has not identified any fundamental issues in the electrical design which would require a significant change to the electrical system design.

33 The Westinghouse Step 4 submission should address all of the issues identified in Section 2.3.2 of this assessment report to enable the GDA assessment of all issues to be addressed.

34 I will carry out an independent assessment of the Westinghouse design to verify its integrity. Westinghouse will be required to provide design data to support this process.

4 REFERENCES

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

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

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

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

5 *AP1000 European Design Control Document.* EPS-GW-GL-700, Revision 0, Westinghouse Electric Company LLC,16 February 2009.

6 *Safety Assessment Principles Roadmap for AP1000 Design.* UKP-GW-GL-741, Revision 0, Westinghouse Electric Company LLC, 26 November 2008.

7 *IEC 61226:2009. Nuclear power plants. Instrumentation and control important to safety. Classification of instrumentation and control functions.* International Electrotechnical Commission (IEC), 2004.

8 *IEEE 741:2000. Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations.* Institute of Electrical and Electronic Engineers (IEEE), 2007.

9 *IEEE 379:2000. Standard Application of the Single Failure Criterion to Nuclear Power Generation Stations Safety Systems.* Institute of Electrical and Electronic Engineers (IEEE), 2000.

10 *Guidelines for Electromagnetic Interference Testing in Power Plants.* EPRI-TR-102323, Revision 1, Electric Research Power Institute (EPRI), 2006.

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

Table 1

Electrical System Safety Assessment Principles Considered During Step 3 Assessment

SAP No.	Assessment topic / SAP title
EKP - Key Principles	
EKP.3	Defence in depth
EKP.5	Safety Measures
EQU - Equipment Qualification	
EQU.1	Qualification procedures
ERL - Reliability Claims	
ERL.2	Measures to achieve reliability
ERL.4	Margins of Conservatism
EMT - Maintenance, inspection and testing	
EMT.1	Identification of requirements
EMT.3	Type testing
EMT.6	Reliability claims
EMT.7	Functional testing
ELO - Layout	
ELO.1	Access
EHA - External and internal hazards	
EHA.10	Electromagnetic interference
EDR, ESS - Failure to safety	
EDR.1	Failure to safety
ESS.21(part)	Reliability – failsafe approach
EKP, EDR, ESS, ERC - Defence in depth	
EKP.3	Defence in depth
EDR.2	Redundancy, diversity and segregation
ESS.2(part)	Determination of safety system requirements – Defence in depth
ESS.7	Diversity in the detection of fault sequences
EDR.3	Common cause failure
EDR.4	Single failure criterion
EKP, ESS, ERL - Safety systems	
EKP.5	Safety Measures

SAP No.	Assessment topic / SAP title
ESS.1	Requirement for safety systems
ESS.2(part)	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.8	Automatic initiation
ESS.9	Time for human intervention
ESS.10	Definition of capability
ESS.11	Demonstration of adequacy
ESS.12	Prevention of service infringement
ESS.15	Alteration of configuration, operational logic or associated data
ESS.16	No dependency on external sources of energy
ESS.19	Dedication to a single task
ESS.20	Avoidance of connections to other systems
ESS.21(part)	Reliability – Avoidance of complexity
ESS.23	Allowance for unavailability of equipment
ESS.24	Minimum operational equipment requirements
EES - Essential services	
EES.1	Provision
EES.2	Sources external to the site
EES.3	Capacity, duration, availability and reliability
EES.4	Sharing with other plants
EES.5	Cross connection with other services
EES.6	Alternative sources
EES.7	Protection devices
EES.8	Sources external to the site – only source
EES.9	Loss of service

Annex 1 – Electrical Systems – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None.				
Regulatory Observations				
RO-AP1000-042	2 Sep 2009	Definition of Electrical Design of AP1000 for GDA	Response dated 1/10/09 details proposals for resolving the points raised in the RO	Step 4

Annex 2 - Assessment against Electrical System Safety Assessment Principles

SAP No.	Main Findings / Observations	Action Required
EQU.1	The claim is that the AP1000 design has addressed EQU.1. However, the justification for the claim is based upon seismic qualification only. Qualification of the electrical systems should also include tests which verify the functionality and performance of equipment prior to entering service and that they will perform the required functions throughout their operational life. Type testing in accordance with recognised international standards is required to demonstrate this.	Westinghouse to describe what approach will be taken with regard to type testing of equipment which has a safety classification. The international standards upon which these tests will be based will also require definition. The distinction between the requirement for type tests and routine tests should also be made clear.
EDR.1	This claim is based upon the benefits offered by the passive safety systems employed. In support of this claim compliance with US nuclear industry codes and standards are referred to such as the NRC General Design Criteria (No 23) *'Protection System Failure Modes'*. The PRA has addressed the reliability of impact of the electrical power supply systems An FMEA for the Class 1E DC and UPS system is provided in Table 8.3.2-7 of the SAPs roadmap document UKP-GW-GL-741 (Ref. 6). The activation and control of certain of the reactor safety systems is dependant upon electrical systems. Both DC and AC electrical systems are employed, but in all cases these systems rely upon the energy storage capacity of DC batteries. These battery backed systems are classified as Class 1E. The AC systems on the nuclear island from which the DC batteries are charged are not formally classified and are referred to as 'non-Class 1E' systems. It is claimed that the onsite AC power system is non-Class 1E and that safety does not depend upon the availability of the main AC system supplies because it supplies only non-safety loads. Thus the requirements of the SAP are met in that failure modes have been formally identified and a Class 1 power system is provided to support the safety functions. However, the case for independence of the DC systems from the AC systems has not been formally made nor has the case for the function of the AC standby generators.	Westinghouse to demonstrate that the reliability of the Class 1E DC system can be achieved. The requirement for classification of the diesel backed AC system as Class 2 should be considered as a means of achieving the required reliability.

SAP No.	Main Findings / Observations	Action Required
EDR.2	For the electrical systems the following claims are made; *"The Class 1E electrical system DC and UPS system is divided into four independent divisions. Any three out of four divisions can shut down the plant safely and maintain it in a safe shutdown condition. Separation criteria preserve the independence of redundant Class 1E circuits as described in DCD subsection 8.3.2.4, and no single credible event is capable of disabling redundant safety-related systems. Special identification criteria are applied for Class 1E equipment, cabling, and raceways as described in DCD subsection 8.3.2.3.'* A key feature of the design is that three out of four divisions are sufficient for all the safety functions to operate. From examination of the design principles it is reasonable to expect a high availability for three battery systems. The provision of the interchangeable spare battery bank is important in this regard by allowing full capacity to be maintained during maintenance. Based upon the above observations I conclude that the requirements of the SAP are met.	Westinghouse to demonstrate how the use of a non classified AC system is compatible with its use in the supply to the static switches of the Class 1E inverters. Westinghouse to demonstrate that the circuit protective measures proposed for the interconnection of the Class 1E battery and the non-Class 1E system assures that the integrity of the Class 1E spare battery cannot be affected. Westinghouse to clarify the term `isolation` as applied to the charger input circuit breaker and demonstrate how this feature helps in maintaining the classification claimed for the two systems that are linked by the circuit breakers.
EDR.3	The results of the PRA are cited as evidence of compliance with EDR.3. The root cause events that were addressed are as follows; Design/manufacturing/construction/installation inadequacy or internal causes. Abnormal environmental stress. Design/manufacturing/construction/installation inadequacy. Also included in this category is the malfunctioning of something internal to the component as a result of normal wear-out or other intrinsic failure and the influence of the normal ambient environment of the component. These root-cause events affect similar components. Maintenance or operation actions were not explicitly modelled. I consider that provisions have been made in the design to provide high reliability through redundancy and diversity and segregation.	Transient overvoltage is a possible common cause failure and we note that transient overvoltage suppression devices are fitted. Westinghouse should justify the philosophy behind the application of overvoltage protection with regard to identified threats, insulation coordination and the susceptibility of connected equipment and so qualify the risk of maloperation. Westinghouse to demonstrate that there is no commonality in the controls for air conditioning within the battery and equipment rooms which could lead to common cause failure. Westinghouse should also demonstrate that segregation within the air handling will prevent a single battery room fire from impacting on the availability of other parts of the safety system supplies

SAP No.	Main Findings / Observations	Action Required
EDR. 4	It is claimed that the AP1000 design has addressed EDR.4 citing the PRA and NRC approval of the AP1000 configuration as evidence to substantiate the claim. The single failure design criteria set down in the US General Design Criteria (GDC 17) is referenced in 8.1.4.2.1 of the DCD Chapter 8.1 (Ref. 5) as being the basis for the design. IEEE 379:2000 (Ref. 9) *'….Single failure criteria to Nuclear Power Station Safety Systems'* is one of a number of US standards quoted as the basis for the design. I consider that the requirements of this SAP are met by the design because of the levels of redundancy within the Class 1E electrical systems.	Westinghouse to verify the justification for the design criteria based on US Standards
ERL.2	The DCD (Ref. 5) describes various measures to ensure the reliability of systems and components. On the basis that the methodology described is implemented within an equivalent standards framework for the UK design, and the design features of the Class 1E system, then I consider that the requirements of the SAP are met. The implementation of the methodology depends upon aspects of design of the electrical scheme and further details are required for assessment during Step 4.	Part of the evidence that measures are applied to achieve reliability is quality assurance. And in this respect standards that are to be applied are important. Westinghouse to provide a comprehensive list of all standards that will be applied to the UK design.
ERL.4	It is claimed that the AP1000 design has addressed ERL.4. The basis for the claim is that *"discussion of multiple safety-related systems is provided throughout the AP1000 PRA"*. The on-site AC system is classified by Westinghouse as a non-safety system and referred to as non-Class 1E. However, failure of the non-class 1E AC system will cause the Class 1E systems to be challenged. Also adverse conditions in the AC systems (such as out of tolerance voltage, or adverse power quality in general) could cause the interface to the Class 1E DC system to malfunction. This raises a consideration that the battery backed AC systems should be designated as Class 2. Due to the lack of classification of the on-site AC system the margins of conservatism with which the on-site AC systems are designed remains unquantified so compliance with this principle needs to be reassessed when the classification of the battery backed AC system has been concluded.	Westinghouse to determine the safety classification of the diesel backed AC system needs to allow a reassessment of the system.

SAP No.	Main Findings / Observations	Action Required
EMT.1	It is claimed in the DCD (Ref. 5) that the AP1000 design has addressed EMT.1. However, the substantiation of the claim does not make reference to the electrical power systems. References in the RP's submission shows that provisions have been made for in-service testing of key items of plant such as the standby diesel generator, auxiliary generators and Class 1E DC batteries, chargers, inverters and Class 1E distribution. A high level assessment of the provisions indicates that they are sufficient to support compliance with the SAP.	The Class 1E DC system is ungrounded but Section 8.3.2.2 of the DCD Chapter 8 refers to ground detection alarms and recognises the need to isolate a single ground fault to prevent a pole-to-pole fault developing. Westinghouse to justify the detection technology used together with its integration into the surveillance strategy. Westinghouse to demonstrate for the ungrounded system the measures to prevent charge accumulation. Westinghouse to demonstrate how the battery surveillance is implemented in relation to the other monitoring and maintenance activity. Information should be supplied to allow the integrity of this system to be assessed. A battery monitoring scheme that involves cell monitoring requires that many sensor wires must be added to the battery rack and many independent sensors used. The upkeep of such a system and the risks presented by the additional wiring on a battery bank can present a considerable challenge in upkeep and maintaining integrity. Westinghouse to provide a safety justification for these issues. Westinghouse to provide a high level statement of maintenance philosophy for the electrical systems. This should include details of maintenance intervals and the requirements for availability of plant items to maintain the required reliability.
EMT.3	For electrical equipment for use in a high integrity system I would expect that type tests should be undertaken in accordance with applicable standards rather than relying upon routine tests with traceability to the type tests. Type tests confirm that the basis for the design has been met and are more comprehensive than routine tests. The RP should be asked to clarify their strategy on where routine tests and type tests are required.	Westinghouse to explain the policy on type testing and routine testing. The type test requirements should be specified for all safety related systems

SAP No.	Main Findings / Observations	Action Required
EMT.6	The testing, maintenance and monitoring provisions are generally focussed on alignment with the reliability design claims on the systems. As a result the approach to maintenance on the on-site AC system reflects the non safety classification assigned to it. For example in DCD Section 8.3.1.1.2.1 (Ref. 5) for the main standby diesel generator *"Maintenance accessibility is provided consistent with the system non safety-related functions and plant availability goals"*. Also in Section 8.3.3 *"Diesel generator operation, inspection, and maintenance in accordance with manufacturers' recommendations".* In conclusion I consider from this high level assessment the provisions for testing, maintaining, and monitoring are consistent with the claims made for the design. However, the lack of classification of the AC system leads, for example, to the application of commercial grade maintenance practices on the standby diesel generators.	
EMT.7	There is no specific information provided regarding the electrical system compliance with this SAP. This will need to be assessed when information is received	Provide a document giving details of functional testing of electrical systems together with justification of compliance with this SAP.
ELO.1	The locations of the key items of safety and safety related electrical plant have been identified in the DCD (Ref. 5) and therefore the requirements of the SAP are met. However, information on the access provisions for operational, maintenance, inspection and testing activities will be required in the Step 4 submission.	Westinghouse to demonstrate that sufficient access provisions for operational, maintenance, inspection and testing activities are provided.
EHA.10	There is a general reference in DCD (Ref. 5) Section 7.1.4.2 that the instrument and control systems are designed in accordance with guidance provided in the applicable portions of EPRI document EPRI-TR-102323, Revision 1, *'Guidelines for Electromagnetic Interference Testing in Power Plants.'* (Ref. 10). Related references are those dealing with grounding (Section 8.3.1.1.7) and lightning protection (Section 8.3.1.1.8). However, these remarks are of a general nature and also the standards referred to do not relate to European practices. Compliance with the European EMC Directive is required for a UK Reactor.	Westinghouse to confirm and document compliance with specific IEC standards covering EMC.

SAP No.	Main Findings / Observations	Action Required
ESS.1	The electrical system architecture is described with the provision of a Class 1E DC system to support the safety systems. The requirements of the SAP have been met for the Class 1 systems but further assessment will be required once the safety classification of the AC systems has been clarified.	
ESS.2	The RP claims compliance with this SAP. In support of the claim it is stated that *"The AP1000 DCD provides specifications, descriptions, analyses results for the safety systems and systems that perform 'defence-in depth functions'".* Example DCD (Ref. 5) references are than given which includes DCD Chapter 8 (the 'safety related' on-site power supplies) and the PRA. The DCD Chapter 8 (8.3.1.1.1) describes supporting loads that have a defence-in-depth function using the standby diesel generator supplies. Section 8.3.1.1.2.1 also has a reference to the on-site diesel generators being Class D defence in depth systems which support non-safety loads. The DCD describes multiple levels of defence to support the safety functions and thus meet the requirements of the SAP.	Westinghouse to provide additional evidence for the claimed relationship between the electrical support for non-safety systems and how this achieves defence in depth.
ESS.3	It is claimed that the SAP has been addressed in Chapter 8 of the DCD (Ref. 5). Each battery bank, including the spare, has a battery monitor system that detects battery open circuit conditions and monitors battery voltage. The battery monitor provides a trouble alarm in the main control room. The battery monitors are not required to support any safety-related function. Monitoring and alarming of DC current and voltage is provided through the plant control system which includes a battery discharge rate alarm (Section 8.3.2.1.1.1). Penetrations carrying medium voltage power cables have thermocouples to monitor the temperature within the assembly at the spot expected to have the hottest temperature. From examination of the monitoring information provided I consider that provisions are proposed which would meet the requirements of a high integrity system.	Westinghouse to provide details of the battery monitoring facilities for assessment. The integrity of the system and its capability to provide adequate monitoring to support the required system reliability needs to be assessed.

SAP No.	Main Findings / Observations	Action Required
ESS.7	It is claimed that the AP1000 design has addressed ESS.7. Areas where protection diversity is applied in the electrical power system is in the provision of two Class 1E HV circuit breakers connected in series feeding each reactor cooling pump and in the multiplicity of circuit protection applied in the Class 1E and non class 1E circuits and equipment. From examination of Chapter 8.3 of the DCD (Ref. 5) the following references to circuit protection are noted. Section 8.1.3.1.1.1.1 describes the HV AC protection relays proposed and refers to the use of differential and overcurrent relays for main and backup protection, multifunction relays on transformer feeders, multifunction motor protection relays and undervoltage relays at medium voltages. LV AC protection is described as including circuit breakers fitted with protection relays and motor control relays. Non-class 1E AC motor operated valves are described as having thermal overload devices selected to minimise the probability of spurious interruptions. Section 8.3.1.1.6 describes primary and backup protective devices protecting Class 1E circuits as Class 1E in accordance with IEEE 741:2000 (Ref. 8). Extensive references are also made to the use of fuses for protection of the Class 1E and non Class 1E DC circuits. From a review of the information contained in the DCD I consider that diversity in protection is applied to the electrical systems and that the SAP requirements are met.	Westinghouse to provide information on the Class 1E AC circuit breakers detailing how the high integrity functionality is achieved. Westinghouse to demonstrate how the verification of software in programmable circuit protection devices is to be applied in order to prove the integrity of these protective devices commensurate with the system classification in which they are applied.
ESS.8	From examination of the DCD (Ref. 5) I consider that the requirements of the SAP are met. All safety loads are supported from the Class 1E power systems and no load transfers are required at the time of a design basis accident and coincident failure of the AC system. No requirement for manual intervention is identified.	

SAP No.	Main Findings / Observations	Action Required
ESS.9	DCD Chapter 6, Sections 6.2 through 6.5 (Ref. 5) provide a description of the engineered safety features. As stated in the response to ESS.8, these safety systems do not normally require human intervention following the start of a requirement for protective action for as long as 3 days. However, in the event of a spurious actuation of a safety system, it is expected that the operator will intervene in accordance with procedures. No human intervention is required or credited, for at least 30 minutes. The requirements of the SAP are met.	
ESS.10	From a high level assessment of the provisions detailed in Chapter 8 of the DCD (Ref. 5) I consider that the requirements of the principle are met for a high integrity system. An aspect of capability which should be further defined during ongoing assessment is the capacity margins that are offered by the vital component parts of the Class 1E system.	Westinghouse to provide information on the capacity margins for the Class 1E batteries at the scheduled loading should be declared taking into account operational uncertainties and degradation.
ESS.11	The principal means of demonstrating the adequacy of the power system are the design calculations. These should include system studies that analyse and confirm performance and allow equipment ratings to be calculated for thermal and short circuit ratings.	Westinghouse to provide a comprehensive range of system studies as the basis for the system design and the determination of plant ratings. These should include load flows, fault studies, protection coordination studies, power quality studies, transient stability including grid stability and insulation coordination studies.
ESS.12	It is claimed that the requirements of this SAP are met. In substantiation reference is made to the fact that the electrical power to the protection and safety monitoring system is provided by batteries. From the assessment of DCD Chapter 8 (Ref. 5) the key approach to preventing infringement of the safety system from the electrical system is through the provision of the Class 1E batteries and of redundancy provisions within the Class 1E scheme. No safety claim is made upon the AC system which feed the battery systems. The classification of the AC system should be clarified in the Step 4 submission.	
ESS.15	Details on programmable devices used in the electrical power system that potentially have an impact on the reactor safety are not described in the DCD (Ref. 5). In order for assessment to be made details on the use of such devices and the control of software production, settings and software versions should be provided.	Westinghouse to identify the use of programmable devices on safety systems. Westinghouse to describe how parameter settings and software versions will be controlled. Where programmable devices are utilised it should be confirmed that networking or other communication is not involved.

SAP No.	Main Findings / Observations	Action Required
	The design for both the AC and DC supplies relies upon conventional and proven key interlocks systems where manual operation could introduce two or more conflicting states. Mechanical interlocks are provided on the HV source incoming breakers on switchgear ES1 and ES2 to prevent inadvertent connection of the onsite standby diesel generator and preferred/maintenance ac power sources to the 11kV buses at the same time. Mechanical interlocks are provided on the 400V load centre bus tie breakers with the corresponding source incoming breakers so that one of the two source incoming breakers must be opened before the associated tie breaker is closed. In the case of a failure or unavailability of the normal battery bank and the battery charger, permanently installed cable connections allow the spare to be connected to the affected bus by plug-in locking type disconnectors along with key interlock switches.	
ESS.16	The AP1000 passive safety systems, once actuated, do not rely on support systems to perform their safety function for at least 3 days. After 3 days, operator action using dedicated, qualified, onsite equipment and stored water, can be used to recharge the 1E batteries to extend the monitoring function of the protection and safety monitoring system, to continue the application of water onto the containment vessel outside surface to augment 'air-only` containment cooling, to direct safety-related stored water to the spent fuel pool, and to re-supply compressed air to maintain the main control room habitability. These operator actions provide at least 4 additional days of safety system operation (1 week total). After 1 week, additional water, fuel, and AC power from offsite sources or use of existing non safety onsite systems can be used to recharge the 1E batteries and re-supply water and air	Westinghouse to provide information on the provision and availability of sources of power to recharge the batteries

SAP No.	Main Findings / Observations	Action Required
ESS.19	From assessment of Chapter 8 of the DCD (Ref. 5) this SAP is met as the Class 1E system is dedicated to the support of safety functions and subject to demonstration of the integrity of the spare Class 1E battery when used as a temporary non-Class 1E replacement. The spare battery can be used as a temporary replacement for the non class 1E battery but interlocks prevent simultaneous use and measures are taken to prevent a non-class 1E system fault damaging the battery.	Westinghouse to demonstrate that the use of the spare battery for temporary replacement of non safety related batteries will not have any effect on the integrity of the safety system.
ESS.20	No connections have been identified between any part of the electrical safety system and any systems external to the plant.	
ESS.21	From a high level assessment of the design it provides the basis for the requirements of this SAP to be met	
ESS.23	It is agreed that the design of the Class 1E and non-Class 1E systems described in the DCD Chapter 8 (Ref. 5) incorporates redundancy and that the design intention is to use the redundancy to facilitate maintenance without compromising system availability. For example the spare battery in the Class 1E system allows maintenance of DC battery and charger without affecting system availability. Analysis has also been presented to confirm that part of the design approach has been to examine and quantify the implication of unavailability of equipment.	Westinghouse to document the requirements for availability of standby and ancillary diesels during reactor operation. This should include statements on maintenance down times and minimum availability requirements for operation.
ESS.24	The minimum configuration of the Class 1E system which is claimed is for 3 Divisions to be operational. The design of the battery systems is adequate to support this requirement. Design load schedules should be presented to confirm load capability.	Westinghouse to document the allowable non availability of diesels as identified for ESS.23.

SAP No.	Main Findings / Observations	Action Required
EES.1	It is claimed that the requirements of this SAP have been met. The reliance upon the Class 1E battery capacity for a post accident period of 3 days, followed by recharge from the on-site ancillary engines to extend the period of support by 4 days, followed by refuelling to extend the post accident period of support to safety systems is claimed to meet the requirement. From the assessment conducted for this and earlier SAPs the question remains as to how the reliability of the ancillary generators, which are proposed as being classified as AP1000 Class D, is assured to support the safety claims made.	Westinghouse to review and justify how the requirements of this SAP are met following the re-classification of the diesel backed AC system in accordance with IEC 61226:2009 (Ref. 7).
EES.2	It is claimed that the requirements of this SAP have been met. The normal source of supply is from the main generator with a back-up from offsite. The offsite supply can be sourced either from the main grid connection or a reserve supply taken from an independent point on the grid. As the external supply is a back up to the site supply the requirements of the SAP are met.	
EES.3	It is claimed that the AP1000 design has addressed EES.3 based upon the provision of electrical supplies for 7 days post accident with the opportunity for refuelling the diesel generators for longer periods.	Westinghouse to demonstrate the integrity of this arrangement in conjunction with the safety classification of the AC system to IEC 61226:2009 (Ref. 7).
EES.4	The basis for the assessment is that it is a single facility with no interconnection or relationship to any other plant and consequently the requirements of the SAP are met.	
EES.5	No cross connections have been identified so the requirements of the SAP have been met.	
EES.6	It is claimed that the requirements of this SAP have been met. A high level assessment of the design shows that the system can support the claims of this SAP.	Westinghouse to provide information on the system studies it has undertaken to ensure that the electrical systems are not affected by adverse conditions in the services to which they provide back up.
EES.7	Assessment of protection devices for the electrical power supply system will be covered in Step 4.	Westinghouse to provide detailed information on the coordination and selection of protection relays and an analysis of their reliability (including common cause failures) particularly for Class 1 and Class 2 systems.
EES.8	There are no sole external electrical supplies to the plant so the requirements of the SAP are met.	

SAP No.	Main Findings / Observations	Action Required
EES.9	Loss of the supplies from the main generator or the alternative sources would initiate start-up of the two standby diesel generators to restore supplies. If the main standby generators fail to start following loss of supply then the supply safety systems remains unaffected because it is sourced from the Class 1E DC batteries. The requirements of the SAP are met by this design.	
EKP.3	It is claimed that the design has addressed the SAP because *"the AP1000 design provides for multiple levels of defence for accident mitigation"*. A detailed description of the multiple levels and how they contribute to defence in depth is given. The reliance only upon DC powered actuators, the fact that this provided by batteries, and the non-reliance upon AC power, is part of the justification for claiming defence-in-depth. Within the design of the power system the explicit claims in Chapter 8 of the DCD (Ref. 5) on defence-in-depth are as follows; Loads that are priority loads for defence-in-depth functions based on their specific functions are assigned to buses ES1 and ES2 which are supported by the standby diesel generators. These plant permanent non safety loads are divided into two functionally redundant load groups. Design provisions to protect the standby diesel generators against overload are implemented in such a way so as not to compromise the on-site power capabilities to support the defence-in-depth loads. The onsite standby diesel generator units and their associated support systems are classified as AP1000 Class D, defence-in-depth systems. From an overview of the electrical power system design the following multiple levels of electrical support to the safety related and safety systems are summarized as follows: There are several sources of HV AC and these are; the main generator, the main point of grid coupling and reserve from an independent point of grid coupling.	

SAP No.	Main Findings / Observations	Action Required
	There are four main HV switchboards on the conventional island, each sourced from two separate transformers and four separate transformer winding windings. Two HV standby power switchboards which support electrical loads that represent system components that enhance an orderly plant shutdown under emergency conditions. Each standby switchboard is supported by a standby generator. The standby generators share a common building but are separated by a 3 hour fire barrier. There are four Divisions of Class 1E DC battery systems which are charged from the AC system and it is upon these electrical systems only that the safety systems are supplied and controlled. Class 1E uninterruptible AC supplies are produced by inverters fed from the Class 1E DC system. There are a total of six Class 1E batteries and associated chargers (excluding a spare). Four batteries are rated to provide 24 hours of post accident support and two batteries are rated to provide 72 hours of post accident support. No manual intervention on the Class 1E electrical support system is required in the first 72 hours post accident. A spare Class 1E battery and charger is kept in a state of charge and can be used to replace any of the batteries in any of the Divisions by key interlocked manual operations. Two LV ancillary generators supply AC power to associated emergency switchboards and from these the Class 1E DC systems can be recharged post accident. Thus 7 days of post accident support is provided by the electrical systems on site. The requirements of the SAP for defence in depth are met.	

SAP No.	Main Findings / Observations	Action Required
EKP.5	Passive safety systems are used that do not require AC power to function. DC power is provided to support reactor trip and engineered safeguards actuation. The batteries are sized to provide power for emergency functions, such as monitoring of post-accident conditions, sufficient for 72 hours. Only after 72 hours is AC power needed to recharge the batteries. From the assessment it is considered that the principle is met by the design of the electrical systems.	