Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 ELECTRICAL SYSTEMS ASSESSMENT OF THE EDF AND AREVA UK EPR

DIVISION 6 ASSESSMENT REPORT NO. AR 09/029-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 EDF and AREVA UK EPR Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the HSE Generic Design Assessment (GDA) process. It provides the results of my GDA Step 3 assessment of electrical engineering by giving an overview of the safety case presented in the PCSR, a description of the standards and criteria adopted in my assessment and a 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) (EDF and AREVA) to provide a PCSR plus topic specific reports. 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.
- Identification of needs for additional regulatory verification/analysis.
- Judging whether the overall design is balanced in terms of the different contributors to overall risk from the plant.

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

- The reliability and availability requirements of the emergency power supply are such that it is not a determining factor in the unavailability of the safety systems to which it supplies power.
- One main emergency diesel generator is provided for each of the four plant divisions and electrical supplies from just one of the four divisions will be sufficient to maintain adequate levels of power to the safety systems.

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 integrity of the electrical system. 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.

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 the:

- Maintenance philosophy.
- DC system design, operation and monitoring.
- Electrical system studies and load flows.
- Electrical protection and relay discrimination.
- Transient stability studies.
- Earthing arrangements for 10kV system.

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

LIST OF ABBREVIATIONS

BMS	(Nuclear Directorate) Business Management System
EA	The Environment Agency
EDF and AREVA	Electricité de France SA and AREVA NP SAS
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
ND	The (HSE) Nuclear Directorate
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
SAP	Safety Assessment Principle
SSC	System, Structure and Component
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 EDF and AREVA 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 sampling of 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 UK EPR design. The SAPs require that electrical system 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 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 UK EPR 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 EDF and AREVA 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 EDF and AREVA design and the Step 3 submission documentation. I have also identified actions agreed with EDF and AREVA to address these observations to enable resolution in time for my Step 4 report.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

4 The main document setting out the EDF and AREVA safety case for electrical systems is the PCSR UK-EPR-0002-132 (Ref. 1). The main claims detailed in this document are:

- The reliability and availability requirements of the emergency power supply are such that it is not a determining factor in the unavailability of the safety systems to which it supplies power.
- One main emergency diesel generator is provided for each of the four divisions and electrical supplies from just one of the four divisions will be sufficient to maintain adequate levels of power to the safety systems.

5 The design and construction of the UK EPR reactor is based on the document RCC-E: 'Design and Construction Rules for Electrical Equipment of Nuclear islands'. This document provides rules covering all aspects of design, construction, installation and commissioning for the electrical systems on the UK EPR reactor.

6 The design details submitted for assessment are based on the UK EPR reactor currently under construction at Flamanville, Normandy, France. Detailed information submitted in support of the documentation provided for the safety case is based on the design of this reactor.

2.2 Standards and Criteria

7 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

8 The EDF and AREVA 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 DC distribution network and electrical protection and controls.

9 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 maintenance and availability of safety systems, electrical protection studies and the use and control of programmable devices (for example governors on diesel alternators and controls on static electrical conversion equipment).

10 More information is required in the EDF and AREVA submission to demonstrate that the detail design meets the safety objectives and that sufficient analysis and engineering substantiation has been performed to prove that the plant will be safe. This will be required to be completed for the Step 4 submission.

11 The EDF and AREVA submission does not provide complete descriptions of system architectures particularly for the DC and UPS systems. This will be required to be completed for Step 4.

2.3.2 Comments on Requesting Party`s Submission

12 The safe operating envelope and operating regime are well established in the EDF and AREVA submission with a clear definition on the required availability of systems to meet the claimed reliability targets. This basis of the design and the methods of operation are fully defined for GDA purposes.

13 The overall architecture of the electrical power system is judged to be well designed with four independent trains each capable of providing the power supplies to maintain the reactor in a safe condition under a wide range of accident conditions. Each of these trains has a standby diesel generator which starts up automatically on loss of voltage on the emergency switchboard busbars. There are also ultimate back up diesel generators on two of the trains which are manually started for maintaining supplies in the unlikely event of a total loss of grid combined with common cause failure of all four standby diesel generators.

14 Full segregation is provided between the electrical systems on each train. EDF and AREVA claim that there are no cross connections which could result in a fault on the electrical system causing adverse effects on other trains. At the level of systems architecture the arguments for this claim has been adequately justified.

15 I have sought clarification from EDF and AREVA on the use of software based programmable control devices on safety related systems and in particular on electrical protection relays and important devices such as diesel governors. These devices will be used for some applications where no alternative relay exists. However, for general applications the design proposals have not been clarified with different practices adopted for the Flamanville EPR compared with other AREVA reactors. For the Step 4 submission

I will require clarification of the extent of the use of programmable devices and evidence of the control measures proposed to ensure the integrity of software design.

16 There are two important claims made by EDF and AREVA 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. EDF and AREVA should supply more evidence on these transients during Step 4.

17 The results of system studies of the electrical system using an acceptable software package are required to be supplied by EDF and AREVA for the Step 4 submission. These will include demonstrations of load flows, fault studies and protection settings to achieve system co-ordination and stability under a wide range of credible accident and fault conditions.

18 The design of the 10KV system proposed by EDF and AREVA is an IT system with an unearthed neutral point. An earth detection system is proposed which would be used for alarm purposes in the event of an earth fault on the 10kV system. The system would continue in operation in the event of a single earth fault. I will require justification for the use of this system and technical details of the earth fault monitoring system proposed as a part of my Step 4 assessment.

19 My assessment against SAP EQU.1 identifies requirements for documentation of design verification requirements for electrical equipment preferably by type testing. I will require a clear statement of requirements for design verification including a distinction between type testing and routine testing.

20 To complete my assessments against a number of the SAPs I require more information to be provided by EDF and AREVA. These requirements are defined against the relevant SAP.

21 I have identified areas for further investigation against SAP EDR.3 which addresses common cause failure. EDF and AREVA should undertake studies to address the potential for and effects of transient overvoltages and the effects of unearthed power systems as part of the Step 4 submission.

22 My assessment against SAP EMT.1 has identified a requirement for a statement of maintenance philosophy including details of maintenance intervals and availability of electrical equipment.

23 A further requirement I have 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.

24 My assessment against SAP EKP.3 which covers defence in depth has identified a system which is well defined to meet the requirements of this SAP.

3 CONCLUSIONS AND RECOMMENDATIONS

25 EDF and AREVA provide adequate claims of compliance for the electrical system architecture defined against the electrical SAPs. In a number of areas more detailed information will be required in the Step 4 submission to provide arguments and evidence in support of the claims.

26 My assessment has not identified any issues in the electrical design requiring changes to the fundamental design of the proposed UK EPR electrical system.

27 The EDF and AREVA Step 4 submission should address all of the issues identified in Section 2.3.2 of this report to enable the GDA assessment of all issues to be addressed.

28 I will carry out an independent assessment of the EDF and AREVA design to verify the integrity of the design. EDF and AREVA will be required to provide design data to support this process.

4 REFERENCES

1 *UK EPR Pre-Construction Safety Report.* UK EPR-0002-132 Issue 02, EDF and AREVA, June 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 *IEC 61000-6-5:2001. Electromagnetic Compatibility (EMC) – Part 6.5 - Generic Standards – Immunity for Power Station and Substation Environments.* International Electrotechnical Commission (IEC), 2001.

6 *IEC 61513:2001. Nuclear power plants. Instrumentation and control for systems important to safety – General requirements for systems.* International Electrotechnical Commission (IEC), 2001.

7 *IEC 62138:2004. Nuclear power plants. Instrumentation and control important for safety – software aspects for computer-based systems performing category B or C functions. I*nternational Electrotechnical Commission (IEC), 2004.

8 *IEC 60880:2006. Nuclear power plants – Instrumentation and control systems important to safety – software aspects for computer-based systems performing category A functions.* International Electrotechnical Commission (IEC), 2006.

9 *RCC-E: Design and Construction Rules for electrical components of PWR nuclear islands.* AFCEN, December 2005 edition.

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				
None.				

Annex 2 - Assessment against Electrical System Safety Assessment Principles

SAP No.	Main Findings / Observations	Action Required
EQU.1	The requirements of this SAP are met for the electrical supply and layout. All safety classified systems and equipment must conform to the Design and Construction Rules for Electrical Equipment of Nuclear Islands (RCC-E) in its entirety. The RCC-E lays down the rules for the qualification procedures to ensure that equipment is suitable for its intended application, service and use. It also defines the identification of the equipment to be qualified and the methods and criteria governing its acceptance. Chapter 3 of the Pre-Construction Safety Report (PCSR) states that electrical equipment qualification can be obtained by testing one or several samples of this equipment against a sequence of conventional representative tests or by a clear demonstration of the capacity of the equipment to operate under defined conditions.	Describe what approach will be taken with regard to type testing of equipment with a safety classification. The distinction between the requirement for type tests and routine tests should also be made clear.
EDR.1	The UK EPR is connected to the 400kV grid at a main connection and an auxiliary connection. The main connection is provided from the generator via a step-up transformer, a coupling circuit breaker and a line circuit breaker. A tapped connection is made between the two circuit breakers to connect two step-down unit transformers. The auxiliary connection is made to an independent point on the grid and feeds an auxiliary step-down transformer similar in rating and construction to the unit transformers. The four trains can be fed from the auxiliary transformer. The power supply to the conventional island comprises four 10kV switchboards fed from the unit transformers. These distribute off-site power through four trains to the nuclear island. The nuclear island has four divisions each with its own distribution train. Each division has a main diesel generator for emergency power supply in the event of the loss of the external power supply. Divisions 1 and 4 each have ultimate back up diesel generators for system black	Provide detailed information to demonstrate the correct coordination of electrical protection and its application to provide timely and selective clearance of electrical faults Section 5.2.2 of the PCSR states that the supply distribution from the uninterruptible power supply (UPS) system in each Division includes *"that required for start-up of the main diesel generators".* EDF and AREVA to demonstrate that the main diesel generators have start up provisions independent of the UPS supplies.

SAP No.	Main Findings / Observations	Action Required
	out. There are also uninterruptible power supplies on each of the four trains. The classification level of the systems, structure or components is used to determine the standard applied in design, manufacture installation and maintenance. The system as designed meets the requirements of the SAP.	
EDR.2	The requirements of this SAP are met. A number of separation redundancy features have been incorporated, the main ones are noted as follows: The electrical structure of the conventional island's high voltage scheme separates the nuclear island's distribution system into four divisions. This results in the creation of four sections each equipped with a main 10 kV switchboard supplied by a unit transformer winding. The allocation of loads to the busbars takes into account the redundancy requirements of the safety systems and the power requirements of the static converters and batteries. The architecture of the supply to the instrumentation and control cabinets and for the switchgear actuation provides adequate redundancy and diversity Each emergency power supply train is installed in a separate division. The separation into divisions ensures that in the event of an internal hazard within a division, only the division in question is affected. Each division has a battery based DC system with charging from the low voltage AC system. The DC system gives 2 hours supply to essential instrumentation and control systems. Each division is supplied by an independent standby diesel generator which is started automatically on loss of voltage on the busbars. Cross connections are provided between divisions for emergency power supplies during maintenance.	Commercial grade UPS tend not to segregate the input, energy charge and storage and output AC production stages and faults in one can often communicate with other parts. The technical specification for UPS systems used in Class 1 or Class 2 systems should be provided for assessment in EDF and AREVA to provide detailed design evidence to demonstrate technical compliance with the claims and arguments for segregation commensurate with the high integrity classification required.

SAP No.	Main Findings / Observations	Action Required
	One train`s power supply is sufficient to maintain the reactor in a safe condition. Only one train should be under maintenance at any time as stated in sub-chapter 3.1 of the PCSR. There are a large number of separation features incorporated in the design which meet the requirements to achieve segregation of the systems in line with the requirements of this SAP.	
EDR.3	Common cause failure has been addressed and the requirements of this SAP are met. The PCSR describes the measures against common cause failure as follows. Particular attention is given to minimizing the possibilities of common cause failures. Physical and spatial separation shall be applied as far as possible. Support functions (energy, control, cooling, etc.) shall be also independent to the largest possible degree. Special emphasis has to be placed on the redundancy and diversity of electrical power supplies. Common cause failure has been addressed for the diesel generators caused by a simultaneous failure of an identical component or the environment (e.g. fuel, temperature, operating conditions). The strategy to combat the risk of common cause failure is reliance on the high intrinsic reliability of the equipment. Two distinct diesel generator designs have been adopted. In addition protection against a common cause failure of the control room cabling due to internal faults is prevented by separation of the main control room cabling from that of the remote shutdown station. The 10kV systems are of the unearthed neutral (I-T) type. It has the advantage that supply may continue even after a first phase to earth fault has occurred. However such a fault must not be allowed to persist indefinitely and difficulties can occur when locating such a fault. Strategies are also required to prevent voltage escalation and degradation due to accumulation of partially degraded insulation.	EDF and AREVA to clarify how risks to the safety of the 10kV system and its integrity are addressed in the event of earth faults on the 10kV system. The comparison should demonstrate why the unearthed approach leads to a quantifiable overall benefit relative to an earthed referenced system taking into account the probability of the event and other forms of segregation and diversity applied in the overall system design. Transient overvoltage is a possible cause of common cause failure. EDFA and AREVA should describe 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.

SAP No.	Main Findings / Observations	Action Required
EDR.4	Assessment of the PCSR shows that the requirements of the SAP are met. Single failures are taken into account for F1A safety classified systems and F1B safety classified functions at the design stage. These failures are random and independent of the initiating event, which necessitate the system operation.The design of structures, systems and components important to safety 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.	
ERL.2	This SAP is met by the framework set out in the RCC-E for qualification of equipment, assessment of manufacture, inspection, testing within a quality assurance system. Within the PCSR there a number of references to facilities provided for in-service maintenance and access whereby systems and equipment are expected to be tested and maintained in accordance with operating experience.	EDF and AREVA to provide details of the proposed policies for the UK EPR for acceptance testing, commissioning, inspection, testing and maintenance of classified electrical systems.
ERL.4	This will be evaluated when the required information is received from the RP.	EDF and AREVA to describe the multiple emergency power supply system component reliabilities, availabilities and lifetime integrities and calculations quantifying the reduction in fault sequence frequency.
EMT.1	The requirements of this principle have been met. The RP has identified a requirement to supply loads such as emergency lighting and the motorised systems required during preventive maintenance operations. These will be supplied by the 400V AC emergency sub-distribution boards. In addition interconnections between the sub-distributions of divisions 1 and 2, and 3 and 4 respectively are closed by manually-controlled fused isolators during maintenance. The provision of a battery monitoring system is proposed which will require to be of sufficient design integrity to ensure the reliability of the battery systems.	The 220V DC system for control rod operation is unearthed. EDF and AREVA should provide details of any earth fault detection technology used together with details of its integration into the surveillance strategy. For the ungrounded system the measures to prevent charge accumulation should be demonstrated. EDF and AREVA should 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

SAP No.	Main Findings / Observations	Action Required
		considerable challenge in upkeep and maintaining integrity. Demonstration is required of the consideration given to these issues. EDF and AREVA should 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	This SAP is met by the requirements in the PCSR Sub-chapter 3.6. The electrical distribution system must be qualified to fulfil its safety role and to withstand the environmental conditions to which it is subjected.	EDF and AREVA to clarify the policy on type testing and routine testing. The type test requirements should be specified for all safety related systems.
EMT.6	The requirements of this SAP have been met in the following statement: Due consideration must be given at the design stage to inspectability and testability of equipment as well as to the possibility of replacement of some equipment, considering that maintenance and testing activities are essential to maintain the safety of the plant throughout operation.	EDF and AREVA should provide technical details to justify the extent and efficiency that the testing provides in revealing defects in classified equipment including the upkeep of the test equipment.
EMT.7	The requirements of this SAP are met by the claim made that the UK EPR design has fully acknowledged the general principle that the in-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component, and the requirement for periodic testing is considered as the most basic requirement for safety classified components.	EDF and AREVA to provide the technical details for implementation of in-service functional testing. Further review will be required to ensure that that carrying out these tests does not cause the loss of any safety function.
ELO.1	The requirements of this SAP have been met. An example is given in the PCSR for maintenance operations that are scheduled around shutdowns.	EDF and AREVA to provide details of equipment layout reviews conducted for the UK EPR electrical systems.

SAP No.	Main Findings / Observations	Action Required
EHA.10	This requirement has been met. An example is given in the PCSR as follows: Cables of various voltages are installed on trays according to their type to avoid electromagnetic interference, as set out in the Table in Section 1.4 of sub chapter 8.4 The lightning protection facilities include additional measures to reduce the electromagnetic effects of currents induced by lightning in locations to be protected, such as building structures, cableways, aerial cables, etc. The RP claims that in order to reduce electromagnetic effects due to lightning or other sources of interference, UK EPR electrical and I&C equipment are designed according to the requirements detailed in the EDF EMC (Immunity) standards and requirements to be specified for electrical equipment. The electromagnetic environment of power stations is defined in the IEC 61000-6-5 Standard (Ref. 5). This document sets immunity requirements for equipment and systems, for which reliable operation is required in the presence of actual electromagnetic conditions. Compliance with these standards is stated to give a high level of confidence in the protection of equipment against electromagnetic interference (EMI): the first ensures that installed equipment will be able to withstand the specified industrial environment and the second ensures that following best practice installation rules will enable satisfactory overall operation of equipment and systems.	Further justification will be provided for the protective measures taken against the effects of electromagnetic interference.

SAP No.	Main Findings / Observations	Action Required
ESS.1	The RP has met this principle by means of a hazard design approach used to determine prevention and protection features to protect the safety systems. The aim is to prevent a hazard from being the cause of the loss of a safety classified function. As a conclusion of the design phase, a fault and protection schedule has been established as part of the safety schedule. It provides a list of all postulated faults with potential unacceptable consequences. It includes all initiating faults, with their frequencies and consequences, the safety systems and beneficial safety-related systems involved, and the overall protection claim. The RP further notes that electrical power supplies are essential as support systems for the reduction of core melt frequency and for the `practical elimination` of high pressure core melt sequences.	
ESS.2	This SAP is met by the use of PSA as an essential part of UK EPR safety and design considerations. The PSA is used to develop the reactor design to assess the relative advantages of different design options within the original project objectives. To be as representative as possible, the PSA also incorporates human reliability assessment, using simplified methods. It also uses component reliability data from French and German or international (EG&G) operating experience and of common mode failure values derived from generic data.	
ESS.3	The SAP has been met by the provision of a central control room with monitoring of operational and safety systems and a remote control point for use in the event of the loss or disabling of the central control room and its instrumentation and control. The control room indicators are used by the operator in managing and monitoring severe accidents.	EDF and AREVA to provide technical descriptions and data to allow full evaluation of this SAP. This should include a schedule of electrical system alarms that are related to safety and the initiation of safety actions and to demonstrate how these support the integrity required of the system
ESS.7	This will be evaluated in Step 4 when the required information is supplied by the RP.	Information should be provided on monitoring variables for the safety related power systems such as current, voltage, frequency, negative sequence components, temperature, partial discharges etc.

SAP No.	Main Findings / Observations	Action Required
ESS.8	The requirements of the SAP have been met by the RP. The submission states that tasks that require a rapid or very reliable response are required to be automated where operational actions required within 30 minutes of an accident to achieve a controlled state or a safe shutdown state. Any reference initiating event requiring operator action within 30 minutes, an adequate level of automatic protection is provided to render the operator action unnecessary.	
ESS.9	The RP has met this SAP by basing the UK EPR design in accordance with the principle that local operator actions on the plant must not be necessary earlier than 1 hour after the operator receives the first significant indication of the occurrence of the event.	
ESS.10	The requirements of the SAP have been met. The RP has described the methods, in the PCSR and associated reference document (RCC-E), by which the emergency diesel generators load ratings and UPS durations are calculated.	EDF ands AREVA to provide more detailed technical information to demonstrate that the ratings exceed by a clear margin the service requirements including loads, duration and all environmental conditions
ESS.11	Chapter C 2000 of the RCC-E document entitled 'Coordination of Electrical Equipment Characteristics' clearly defines the design principles to achieve a rating specification for all the electrical equipment including those in essential systems, and emergency diesels and ultimate diesels. The aspects dealt with in the chapter includes the coordination of steady state and transient voltage levels, system earthing, insulation coordination, isolation, fault levels, equipment rating, protection coordination, and generator sizing.	EDF and AREVA to provide a fault and protection schedule for review. A comprehensive range of system studies should be provided 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	This SAP has been met by the provision of safeguards such as the interconnections between train power systems during maintenance plus the redundancy and independence of each division.	

SAP No.	Main Findings / Observations	Action Required
ESS.15	Both AC (HV and LV) and DC electrical switchboards can be supplied by two different electrical sources. To prevent conflicting electrical states, a system based on key interlocks prevents simultaneous supply by both electrical sources. Chapter C5000 of RCC-E entitled 'Programmable Systems' details the standards (IEC 61513, IEC 60880, IEC 62138 – Refs 6, 8 and 7) to be applied with respect to program development, contribution to reliability, availability, maintainability and safety; specification, safety class functions, design, validation, configuration management and integration.	EDF and AREVA to identify and then justify the use of programmable devices on safety systems. Demonstration should be provided of 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. The control of programmable devices for use on safety systems needs to be addressed and subject to assessment.
ESS.16	The RP has met this principle by the incorporation of emergency diesel generators, station blackout diesel generators and battery based uninterruptible power supplies to back-up the two external sources of electricity supply. Thus no sources of external supply are required to maintain a safe state.	
ESS.19	The UK EPR design meets this SAP for the electrical power supply systems since there is no safety or safety related systems present that have more than one function or could be affected by a conflict between two or more separate functions.	
ESS.20	No external connections have been identified (via the protection relays or other safety systems) during the assessment and the requirements of the SAP are met.	EDF and AREVA to provide additional analysis for this SAP should programmable devices be embedded in electrical power system control devices.
ESS.21	From a high level assessment of the design it provides the basis for the requirements of this SAP to be met.	Demonstration should be provided that the detailed requirements of this SAP are met
ESS.23	This SAP has been met by the use of 4 divisions with associated independent emergency power systems with the capability of backing each other up by interconnections. Each of the divisions of the electrical power systems is capable of maintaining the reactor in a safe state without the availability of any other division. It has also been met by the redundancy provided in the unit transformers, auxiliary transformers, emergency diesel generators and ultimate emergency generators.	

SAP No.	Main Findings / Observations	Action Required
ESS.24	This SAP has been met as it has been stated that the electrical equipment provided by one division is adequate to support a safe reactor shutdown.	
EES.1	Electrical supplies are provided through four separate divisions to meet the normal auxiliary power requirements of the reactor, with one division alone being sufficient. The source of supply is normally from the main grid connection. Emergency electrical supplies are provided by one emergency generator in each division with on-site storage facilities for fuel. Battery systems provide support to safety systems in the event that the normal and emergency sources of supply fail and provide a 2 hour window for the start-up the Ultimate diesel generators to be manually initiated. The requirements of this SAP have been met.	Details should be supplied for assessment of the capacity of the key energy storage reserves upon which the design depends and the margins of reserve they provide. For example diesel fuel tank capacities and predicted consumption should be provided to meet target durations**.**
EES.2	Electrical supplies from external to the site are backed up by the emergency diesel generators, battery based uninterruptible supplies, and ultimate diesel generators. Therefore, the requirements of this SAP for back up sources of supply on site are met by the design.	
EES.3	The requirements for back up supplies will be assessed following receipt of details from the RP.	EDF and AREVA to provide data and calculations to confirm that the rating of each back-up source is adequate with sufficient safety margins allowed and under the specified range of environmental conditions.
EES.4	This SAP is met since the basis of the UK EPR design is for a single facility with no interconnection or relationship to any other plant.	
EES.5	This SAP has been met in the UK EPR design by the avoidance of any cross-connections between essential services for safety functions and essential services for non-safety functions.	
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.	System studies will be carried out to ensure that the electrical systems are not affected by adverse conditions in the services to which they provide back up.

SAP No.	Main Findings / Observations	Action Required
EES.7	Assessment of protection devices for the electrical power supply system will be covered on receipt of information from the RP	EDF and AREVA to provide detail information on the coordination and selection of protection relays and an analysis of their reliability (including common cause failures) particularly for F1A and F1B systems.
EES.8	This SAP is not applicable since the UK EPR design does not incorporate an external source of essential services as the only source.	
EES.9	This SAP has been met by defence in depth and the use of 4 independent trains to ensure that the loss of the normal service plus one back-up service does not prevent safety functions from being carried out.	
EKP.3	The RP has met the requirements of this SAP as described in Chapter 3.1 of the PCSR. The safety approach at the design level is based on the concept of defence in depth. The defence in depth has a 5-level structure as required by International Atomic Energy Agency (IAEA) Safety Guide: The implementation of the multiple levels of defence to the electrical system is summarized in the following provisions: A normal source of supply from the 400kV point of coupling to the utility grid within the power station main substation. This point of supply can be derived from either the main station alternator or the grid alone. 400kV Circuit breakers control this power flow and selection. The main generator is connected to the generator step-up transformer via the main power transformer (TP) secondary circuit breaker. Two step-down transformers (TS) each with two secondaries provide galvanically separate supplies to each of four trains via four main switchboards on the conventional island. One train is sufficient to support the safety functions.	

SAP No.	Main Findings / Observations	Action Required
	An auxiliary transformer (TA), identically rated to the TS, supplied from a reserve source of grid supply taken from an alternative point of grid coupling, that is independent of the main point of coupling allows certain auxiliaries to be supplied during shutdown in normal or accident conditions. Each emergency power supply system is installed in a separate division. The separation is such that an internal hazard within one division does not affect that in another division. Automatic and manual transfer from the TS to TA is provided. The three transformers are located on the edge of the conventional island and cable interconnectors to the conventional island HV switchboards in the electrical building, are kept separate. The nuclear island main switchboards are located in fire segregated areas. Each of the emergency switchboards is supported by a 10kV diesel generator. The Diesel Generator buildings are geographically separated so that a single incident can only make two main diesels and one ultimate diesel unavailable. From the emergency switchboard in each train, 690V and 400V switchboards supply power to safety related auxiliaries. In each Division (Train) a UPS with a 2 hour autonomy supplies Controls and Instrumentation (C&I). In Division 1 and 4 there are post accident UPS with 12 hour autonomy for management of severe accidents. The 2 hour and 12 hour uninterruptible inverters are provided with a bypass via a 500kVA transformer regulator.	

SAP No.	Main Findings / Observations	Action Required
	There are two Ultimate Diesel Generators with 24-hour capacity to supply a number of the 690V actuators and the UPS supplies in Divisions 1 and 4. The Ultimate diesels supply all the 690V load required in the event of blackout in order to fulfill safety functions. One Ultimate Diesel Generator is sufficient to protect against plant blackout. Interlocked cross connection is provided between Divisions 1 and 2 and between Divisions 3 and 4 at the 690V and 400V levels so that power can be provided other divisions during plant maintenance.	
EKP.5	This SAP is met based upon the provisions made in the design of the electrical systems as described in the PCSR. A 2 hour battery backed uninterruptible power system in each Division is provided to support safety functions and a 12 hour battery back severe accident power system provides power to safety functions. The emergency generators (one per Division) act as a first line of defence to support safety related loads. These generators are automatically started on loss of bus voltage. For loss of emergency generators and incoming supplies longer than 2 hours two manually started ultimate diesels provide longer duration support and battery recharge. Other design safety measures include segregation of equipment between Divisions, cable segregation linking between Divisions, and provision for maintenance through interconnections between Divisions.	EDF and AREVA to provide detailed design submissions to justify the safety measures to support the integrity of the electrical system.